Microsoft

AZ-400
Microsoft Azure DevOps Solutions

Total Questions: 200

Latest Version

Topic 1, Case Study: 1
Overview

Existing Environment

Litware, Inc. an independent software vendor (ISV) Litware has a main office and five branch offices.

Application Architecture

The company' s primary application is a single monolithic retirement fund management system based on ASP.NE T web forms that use logic written in V8.NET. Some new sections of the application are written in C#.

Variations of the application are created for individual customers. Currently, there are more than 80 have code branches in the application's code base.

The application was developed by using Microsoft Visual Studio. Source code is stored in Team Foundation Server (TFS) in the main office. The branch offices access of the source code by using TFS proxy servers.

Architectural Issues

Litware focuses on writing new code for customers. No resources are provided to refactor or remove existing code. Changes to the code base take a long time, AS dependencies are not obvious to individual developers.

Merge operations of the code often take months and involve many developers. Code merging frequently introduces bugs that are difficult to locate and resolve.

Customers report that ownership costs of the retirement fund management system increase continually. The need to merge unrelated code makes even minor code changes expensive.

Requirements

Planned Changes

Litware plans to develop a new suite of applications for investment planning. The investment planning Applications will require only minor integration with the easting retirement fund management system.

The investment planning applications suite will include one multi-tier web application and two iOS mobile applications. One mobile application will be used by employees; the other will be used by customers.

Litware plans to move to a more agile development methodology. Shared code will be extracted into a series of package.

Litware has started an internal cloud transformation process and plans to use cloud based services whenever suitable.

Litware wants to become proactive m detecting failures, rather than always waning for customer bug reports.

Technical Requirements

The company's investment planning applications suite must meet the following technical requirements:

• New incoming connections through the firewall must be minimized.

• Members of a group named Developers must be able to install packages.

• The principle of least privilege must be used for all permission assignments

• A branching strategy that supports developing new functionality in isolation must be used.

• Members of a group named Team leaders must be able to create new packages and edit the permissions of package feeds

• Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use.

• By default, all App Center must be used to centralize the reporting of mobile application crashes and device types in use.

• Code quality and release quality are critical. During release, deployments must not proceed between stages if any active bugs are logged against the release.

• The mobile applications must be able to call the share pricing service of the existing retirement fund management system. Until the system is upgraded, the service will only support basic authentication over HUPS.

• The required operating system configuration tor the test servers changes weekly. Azure Automation State Configuration must be used to ensure that the operating system on each test servers configured the same way when the servers are created and checked periodically.

Current Technical

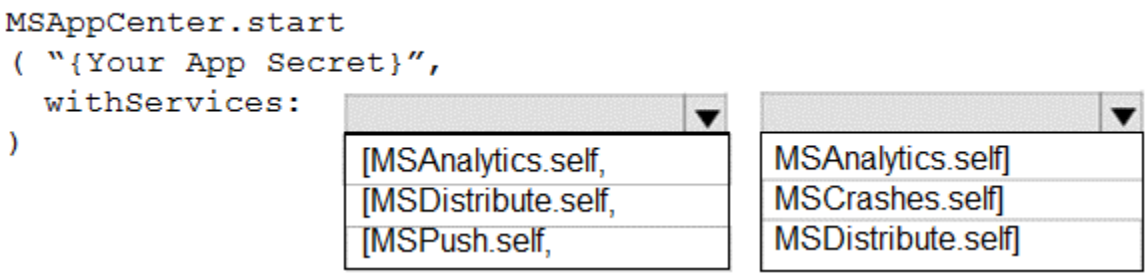
The test servers are configured correctly when first deployed, but they experience configuration drift over time. Azure Automation State Configuration fails to correct the configurations.

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

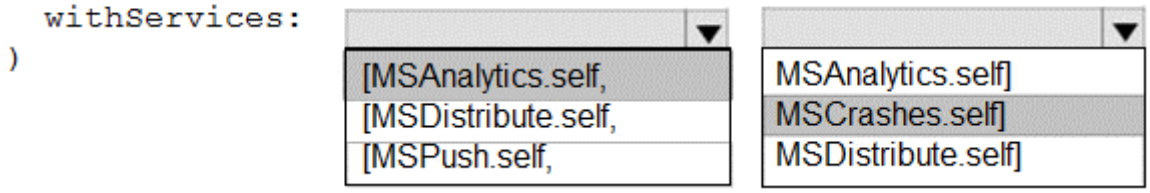
```
Register-AzureRmAutomationDscNode
  -ResourceGroupName 'TestResourceGroup'
  -AutomationAccountName 'LitwareAutomationAccount'
  -AzureVMName $vmanme
  -ConfigurationMode 'ApplyOnly'
```

Question: 1

How should you complete the code to initialize App Center in the mobile application? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection a worth one point.



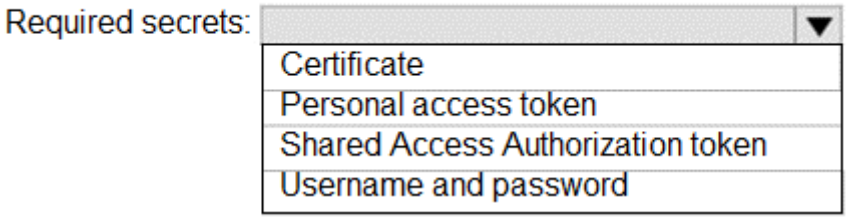
Answer:

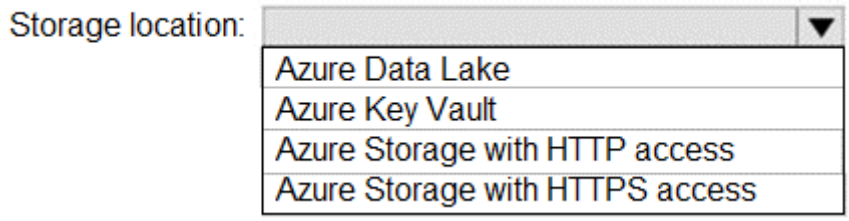


Explanation:
Scenario: Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use.
In order to use App Center, you need to opt in to the service(s) that you want to use, meaning by default no services are started and you will have to explicitly call each of them when starting the SDK.
Insert the following line to start the SDK in your app's AppDelegate class in the didFinishLaunchingWithOptions method.
MSAppCenter.start("{Your App Secret}", withServices: [MSAnalytics.self, MSCrashes.self])
References: https://docs.microsoft.com/en-us/appcenter/sdk/getting-started/ios

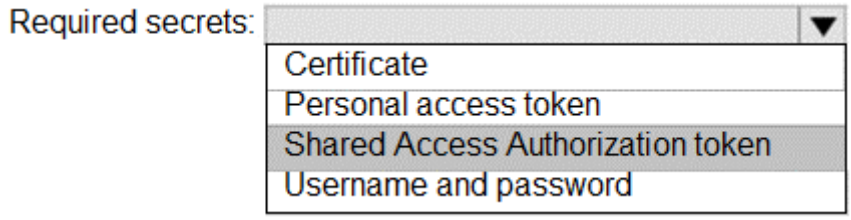
Question: 2

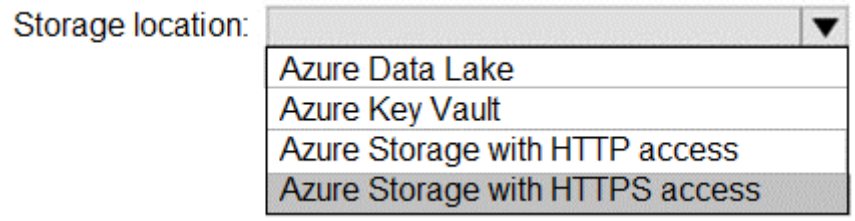
How should you confrere the release retention policy for the investment planning depletions suite? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.





Answer:

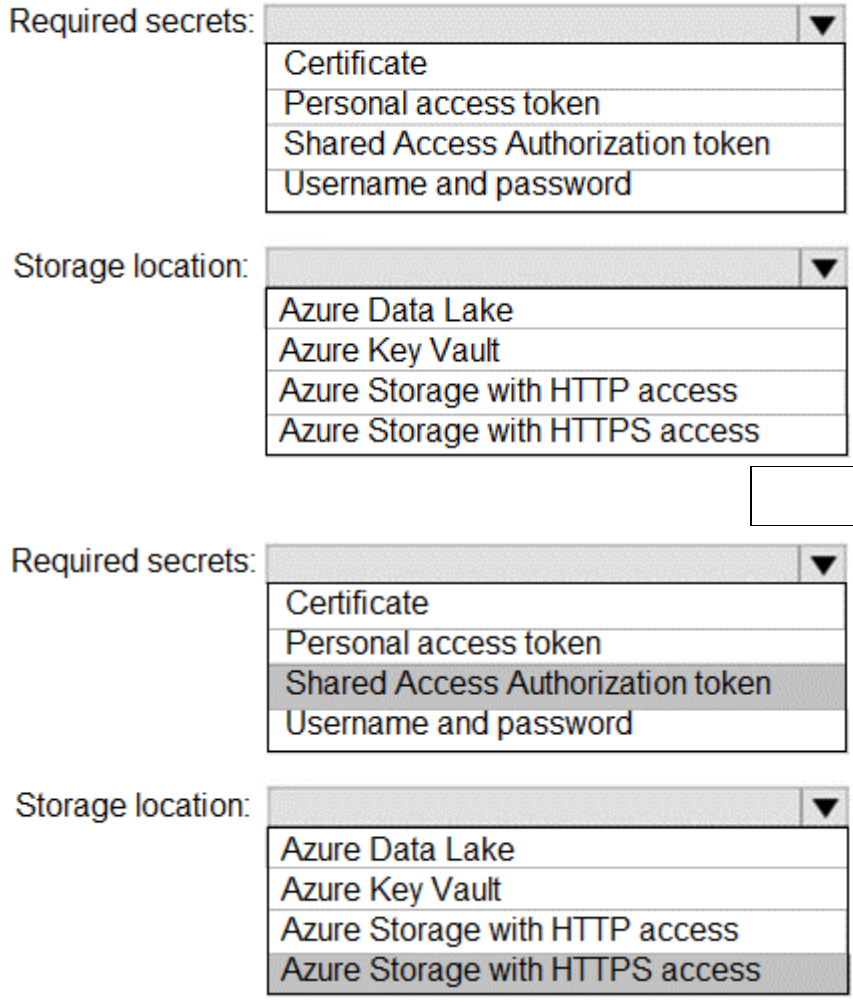




Explanation:
Every request made against a storage service must be authorized, unless the request is for a blob or container resource that has been made available for public or signed access. One option for authorizing a request is by using Shared Key.
Scenario: The mobile applications must be able to call the share pricing service of the existing retirement fund management system. Until the system is upgraded, the service will only support basic authentication over HTTPS.
The investment planning applications suite will include one multi-tier web application and two iOS mobile application. One mobile application will be used by employees; the other will be used by customers.
References: https://docs.microsoft.com/en-us/rest/api/storageservices/authorize-with-shared-key

Question: 3

You need to configure a cloud service to store the secrets required by the mobile applications to call the share.
What should you include in the solution? To answer, select the appropriate options m the answer ate», NOTE: Each correct selection is worth one point.



Answer:

Explanation:
Every request made against a storage service must be authorized, unless the request is for a blob or container resource that has been made available for public or signed access. One option for authorizing a request is by using Shared Key.
Scenario: The mobile applications must be able to call the share pricing service of the existing retirement fund management system. Until the system is upgraded, the service will only support basic authentication over HTTPS.
The investment planning applications suite will include one multi-tier web application and two iOS mobile application. One mobile application will be used by employees; the other will be used by customers.
References: https://docs.microsoft.com/en-us/rest/api/storageservices/authorize-with-shared-key

Question: 4

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 $vmanme
   -ConfigurationMode 'ApplyOnly'
```

References: https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode?view=azurermps-6.13.0

Question: 5

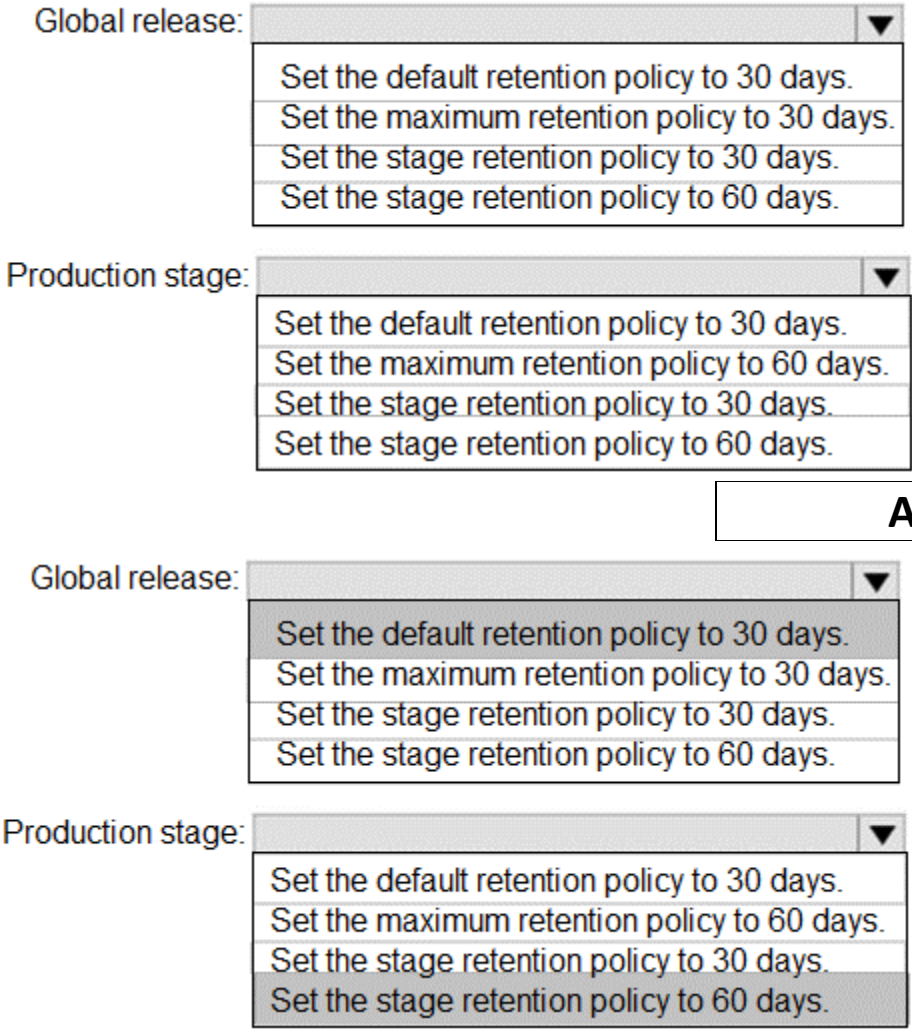
What should you use to implement the code quality restriction on the release pipeline for the investment planning applications suite?

A. a trigger
B. a pre deployment approval
C. a post-deployment approval
D. a deployment gate

Answer: D

Question: 6

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.

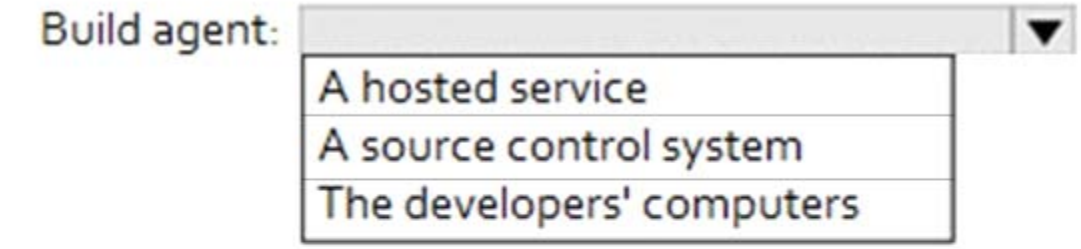


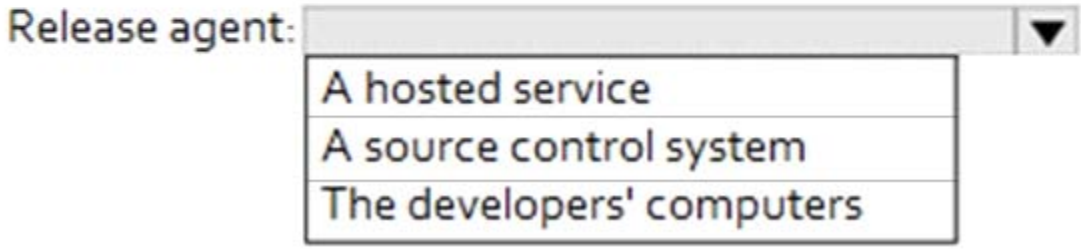
Answer:

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/en-us/azure/devops/pipelines/policies/retention

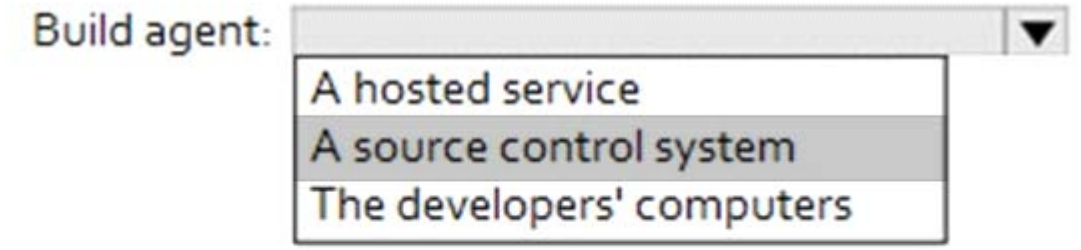
Question: 7

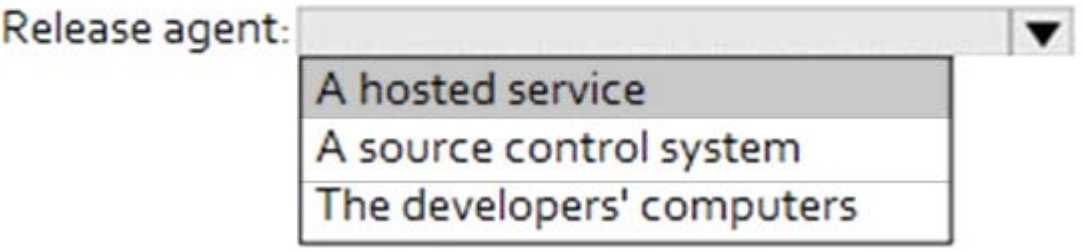
Where should the build and release agents for the investment planning application suite run? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.





Answer:





Explanation:
Box 1: A source control system
A source control system, also called a version control system, allows developers to collaborate on code and track changes. Source control is an essential tool for multi-developer projects.
Box 2: A hosted service
To build and deploy Xcode apps or Xamarin.iOS projects, you'll need at least one macOS agent. If your pipelines are in Azure Pipelines and a Microsoft-hosted agent meets your needs, you can skip setting up a self-hosted macOS agent.
Scenario: The investment planning applications suite will include one multi-tier web application and two iOS mobile applications. One mobile application will be used by employees; the other will be used by customers.
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-osx?view=azure-devops

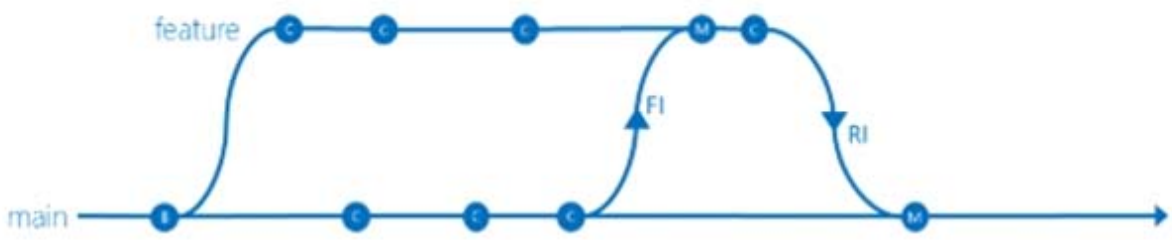
Question: 8

Which branching strategy should you recommend for the investment planning applications suite?

A. release isolation
B. main only
C. development isolation
D. feature isolation

Answer: C

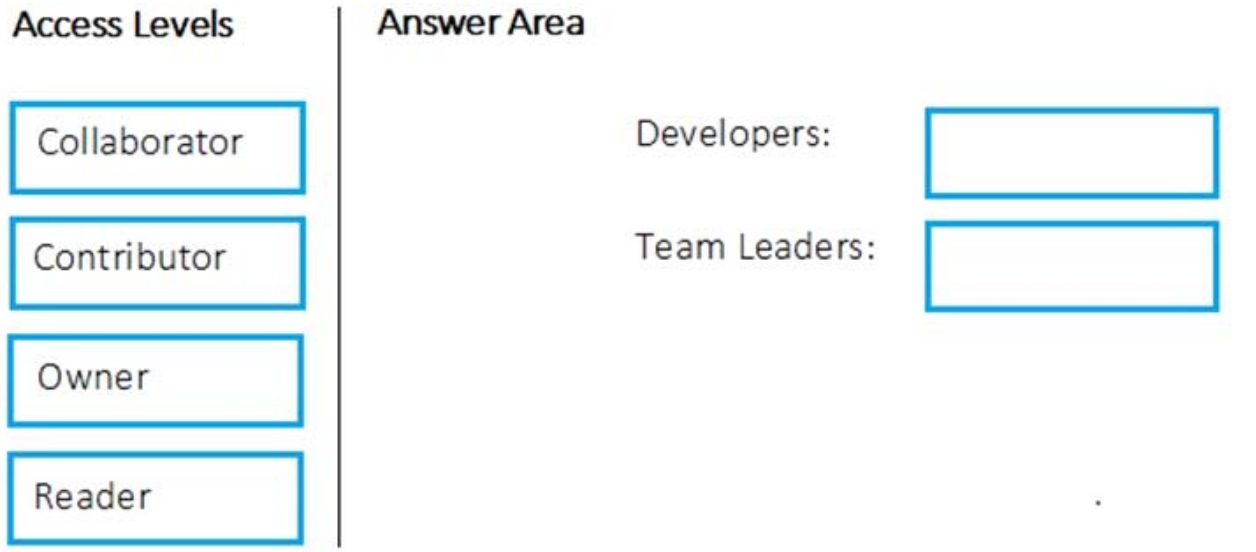
Explanation:
Scenario: A branching strategy that supports developing new functionality in isolation must be used.
Feature isolation is a special derivation of the development isolation, allowing you to branch one or more feature branches from main, as shown, or from your dev branches.



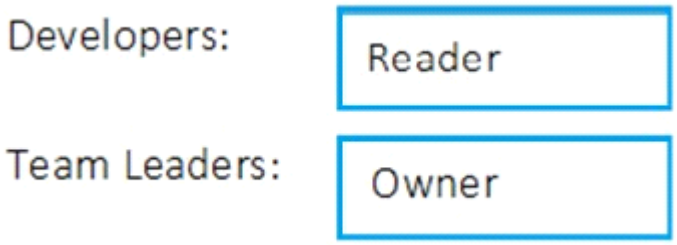
When you need to work on a particular feature, it might be a good idea to create a feature branch.
Incorrect Answers:
A: Release isolation introduces one or more release branches from main. The strategy allows concurrent release management, multiple and parallel releases, and codebase snapshots at release time.
B: The Main Only strategy can be folder-based or with the main folder converted to a Branch, to enable additional visibility features. You commit your changes to the main branch and optionally indicate development and release milestones with labels.
C: Development isolation: When you need to maintain and protect a stable main branch, you can branch one or more dev branches from main. It enables isolation and concurrent development. Work can be isolated in development branches by feature, organization, or temporary collaboration.
References:
https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/branching-strategies-with-tfvc?view=azure-devops

Question: 9

Which package feed access levels should be assigned to the Developers and Team Leaders groups for the investment planning applications suite? To answer, drag the appropriate access levels to the correct groups. Each access level 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.



Answer:



Explanation:
Box 1: Reader
Members of a group named Developers must be able to install packages.
Feeds have four levels of access: Owners, Contributors, Collaborators, and Readers. Owners can add any type of identity-individuals, teams, and groups-to any access level.
Box 2: Owner
Members of a group named Team Leaders must be able to create new packages and edit the permissions of package feeds.

Permission	Reader	Collaborator	Contributor	Owner
List and restore/install packages	✓	✓	✓	✓
Save packages from upstream sources		✓	✓	✓
Push packages			✓	✓
Unlist/deprecate packages			✓	✓
Delete/unpublish package				✓
Edit feed permissions				✓
Rename and delete feed				✓

Topic 3, Case Study: 2

Overview

Existing Environment

Contoso, Ltd. is a manufacturing company that has a main office in Chicago.

Requirements

Contoso plans to improve its IT development and operations processes implementing Azue DevOps principles. Contoso has an Azure subscription and creates an Azure DevOPs organization.

The Azure DevOps organization includes:

- The Docker extension
- A deployment pool named Pool7 that contains 10 Azure virtual machines that run Windows Server 2016.

The Azure subscription contains an Azure Automation account.

Planned Changes

Contoso plans to create projects in Azure DevOps as shown in the following table.

Project name	Project details
Project 1	Project1 will provide support for incremental builds and third-party SDK components
Project 2	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.
Project 3	Project3 will be integrated with SonarQube
Project 4	Project4 will provide support for a build pipeline that creates a Docker image and pushes the image to the Azure Container Registry. Project4 will use an existing Dockerfile.
Project 5	Project5 will contain a Git repository in Azure Reports and a continuous integration trigger that will initiate a build in response to any change except for changes within /folder1 of the repository.
Project 6	Project6 will provide support for build and deployment pipelines. Deployment will be allowed only if the number of current work items representing active software bugs is 0.
Project 7	Project7 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.

Technical Requirements

Contoso identities the following technical requirements:

• Implement build agents rot Project 1.

• Whenever possible, use Azure resources

•Avoid using deprecated technologies

• Implement a code flow strategy for Project2 that will:

•Enable Team 2 to submit pull requests for Project2.

• Enable Team 2 to work independently on changes to a copy of Project?

• Ensure that any intermediary changes performed by Tram2 on a copy of Project2 will be subject to the same restrictions as the ones defied in the build policy of Project2.

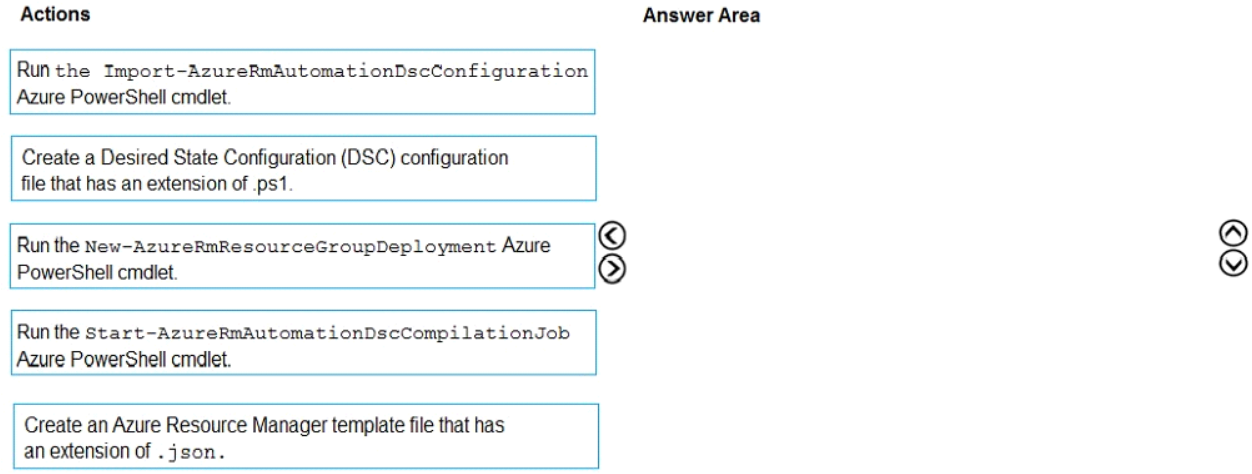
• Whenever possible. Implement automation and minimize administrative effort.

• Implement Protect3, Project5, Project6, and Project7 based on the planned changes.

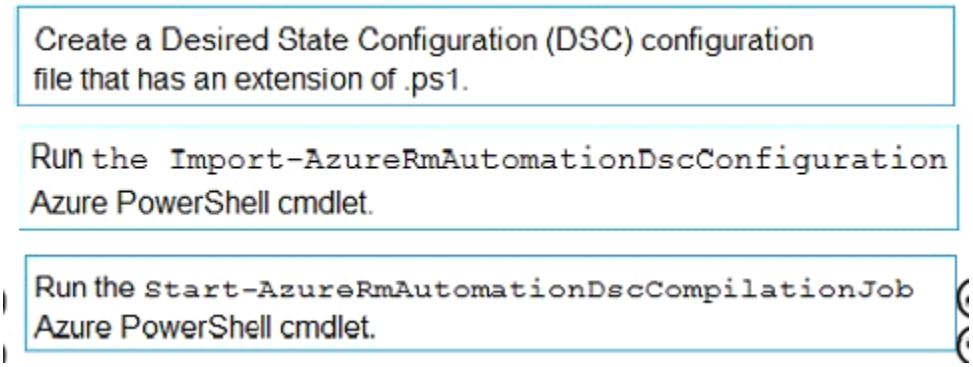
• Implement Project4 and configure the project to push Docker images to Azure Container Reentry.

Question: 10

You need to configure Azure Automation for the computer in Group7.
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.



Answer:



Explanation:
Step 1: Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1.
Step 2: Run the Import-AzureRmAutomationDscConfiguration Azure Powershell cmdlet
The Import-AzureRmAutomationDscConfiguration cmdlet imports an APS Desired State Configuration (DSC) configuration into Azure Automation. Specify the path of an APS script that contains a single DSC configuration.
Example:
PS C:\>Import-AzureRmAutomationDscConfiguration -AutomationAccountName "Contoso17"-ResourceGroupName "ResourceGroup01" -SourcePath "C:\DSC\client.ps1" -Force
This command imports the DSC configuration in the file named client.ps1 into the Automation account named Contoso17. The command specifies the Force parameter. If there is an existing DSC configuration, this command replaces it.
Step 3: Run the Start-AzureRmAutomationDscCompilationJob Azure Powershell cmdlet
The Start-AzureRmAutomationDscCompilationJob cmdlet compiles an APS Desired State Configuration (DSC) configuration in Azure Automation.
References:

https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/import-azurermautomationdscconfiguration
https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/start-azurermautomationdsccompilationjob

Question: 11

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	Project7 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/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode

Question: 12

In Azure DevOps, you create Project3.
You need to meet the requirements of the project.
What should you do first?

A. From Azure DevOps, create a service endpoint.
B. From SonarQube, obtain an authentication token.
C. From Azure DevOps, modify the build definition.
D. From SonarQube, create a project.

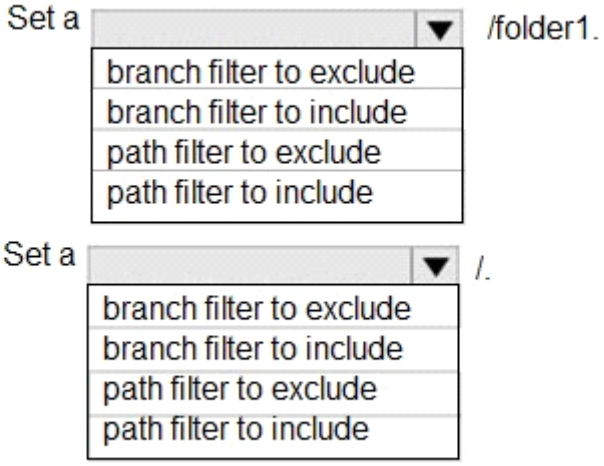
Answer: A

Explanation:
The first thing to do is to declare your SonarQube server as a service endpoint in your VSTS/DevOps project settings.

References: https://docs.sonarqube.org/display/SCAN/Analyzing+with+SonarQube+Extension+for+vsts-TFS

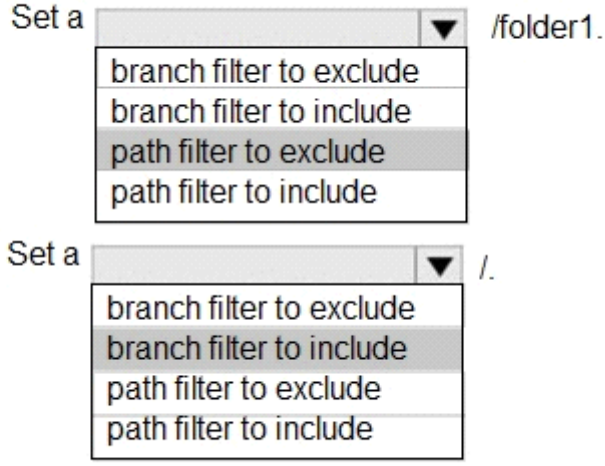
Question: 13

How should you configure the filters for the Project5 trigger? To answer, select the appropriate option in the answer area.
NOTE: Each correct selection is worth one point.



@

Answer:



@

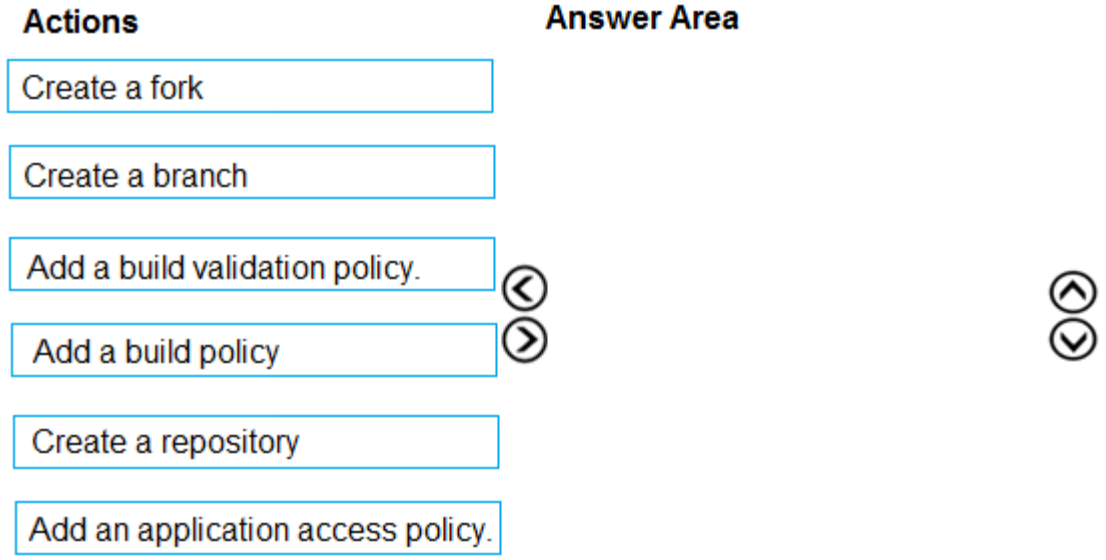
Explanation:
Scenario:

Project5 will contain a Git repository in Azure Reports and a continuous integration trigger that will initiate a build in response to any change except for changes within /folder1 of the repository.

References: https://docs.microsoft.com/en-us/azure/devops/pipelines/build/triggers

Question: 14

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.



Answer:

Answer Area

Create a repository
Create a branch
Add a build validation policy.

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.

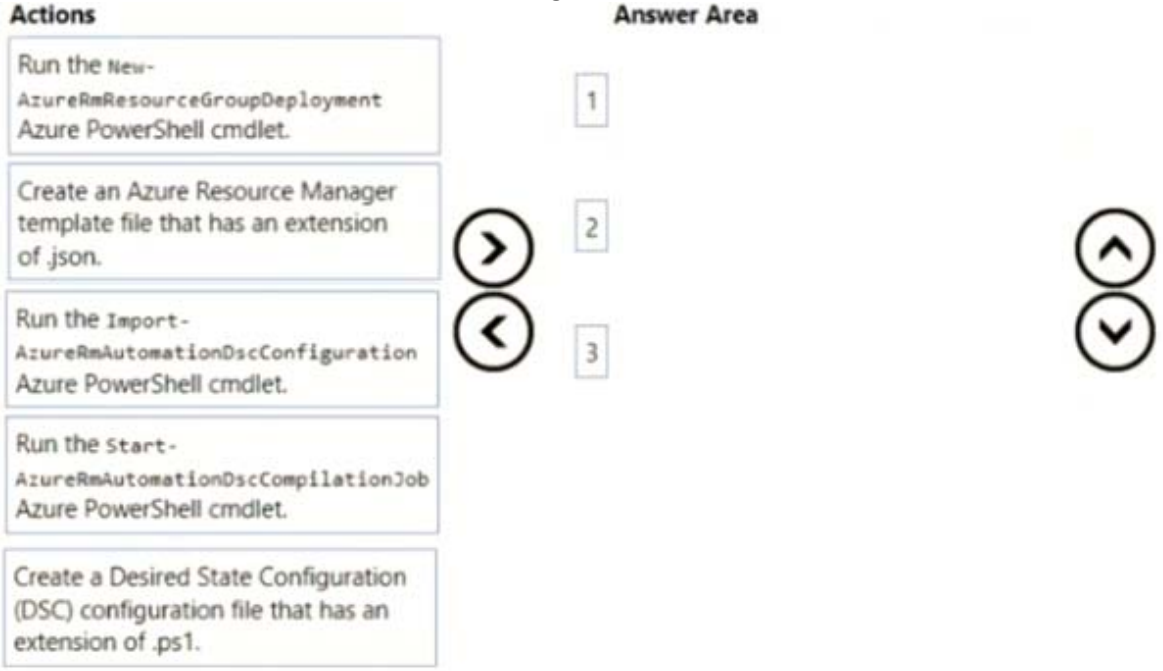
Ensure that any intermediary changes performed by Team2 on a copy of Project2 will be subject to the same restrictions as the ones defined in the build policy of Project2.

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.

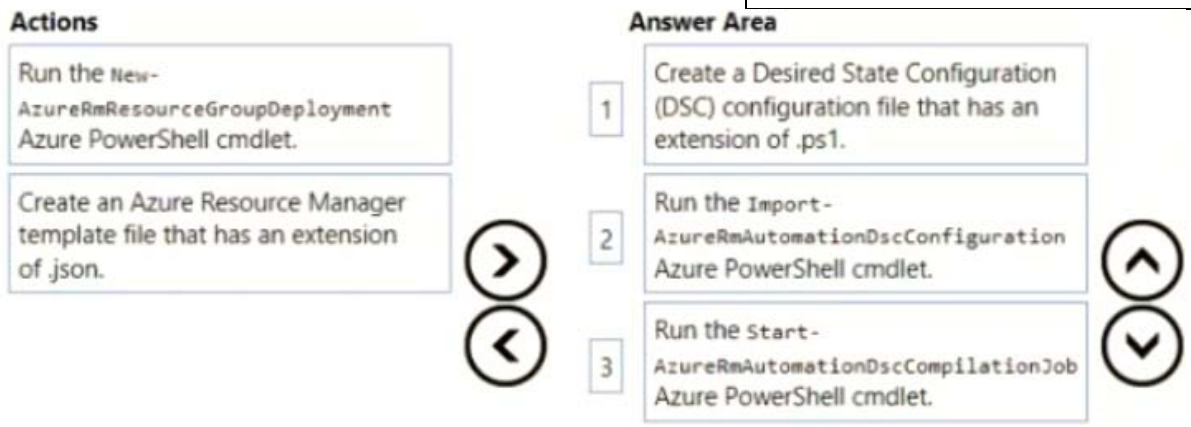
References: https://docs.microsoft.com/en-us/azure/devops/repos/git/manage-your-branches

Question: 15

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 m the correct order.



Answer:



Question: 16

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 m the correct order.

Answer:

Open the release pipeline editor.

Enable Gates.

Add Query Work Items.

Explanation:

Scenario: Implement Project3, Project5, Project6, and Project7 based on the planned changes

Project 6	Project6 will provide support for build and deployment pipelines. Deployment will be allowed only if the number of current work items representing active software bugs is 0.

Step 1: Open the release pipeline editor.

In the Releases tab of Azure Pipelines, select your release pipeline and choose Edit to open the pipeline editor.

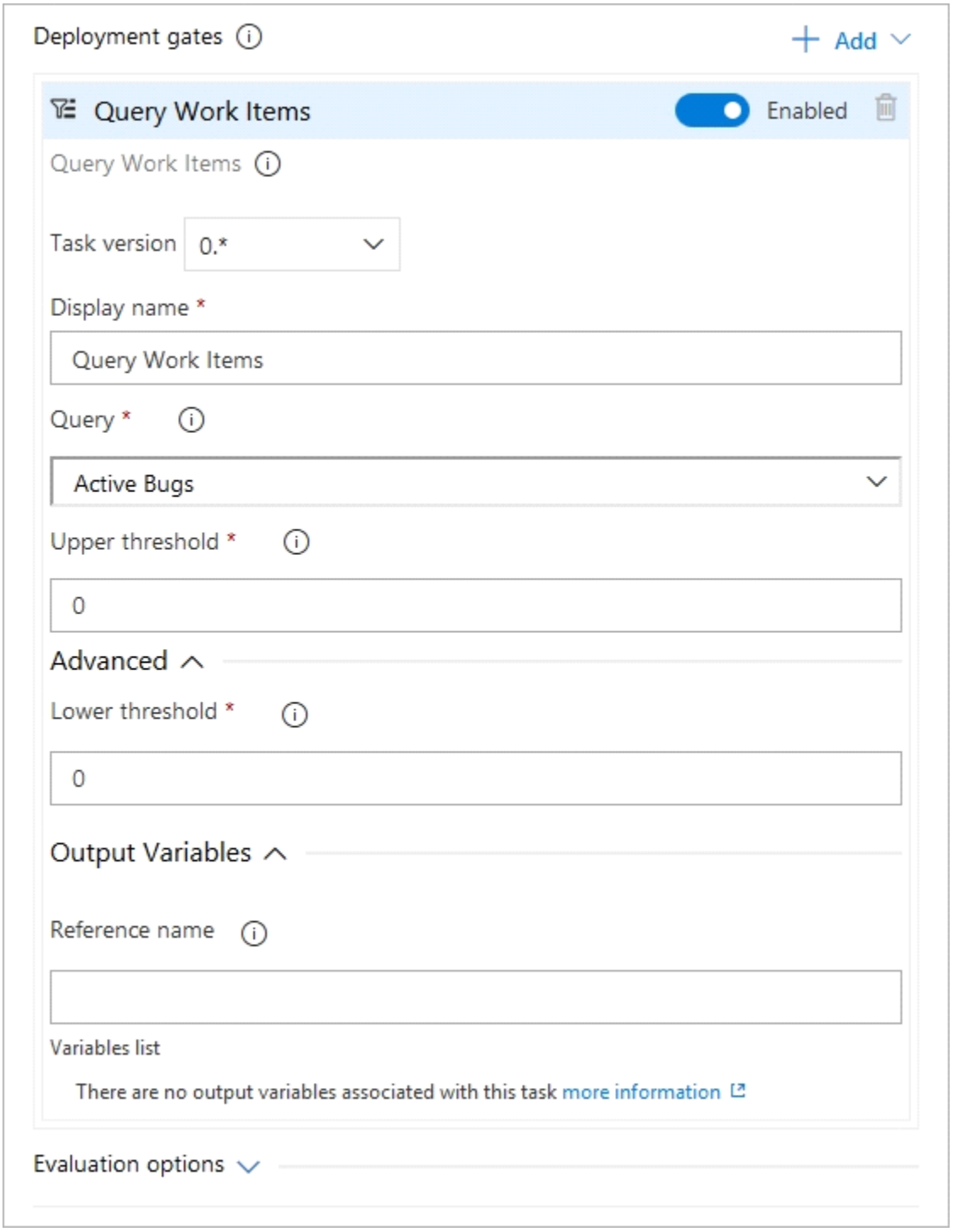
Step 2: Enable Gates.

Choose the pre-deployment conditions icon for the Production stage to open the conditions panel. Enable gates by using the switch control in the Gates section.

Step 3: Add Query Work items.

Choose + Add and select the Query Work Items gate.

Configure the gate by selecting an existing work item query.



Note: A case for release gate is:
Incident and issues management. Ensure the required status for work items, incidents, and issues. For example, ensure deployment occurs only if no priority zero bugs exist, and validation that there are no active incidents takes place after deployment.
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deploy-using-approvals?view=azure-devops#configure-gate

Question: 17

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 them in the correct order.

Actions

- Create a repository
- Add a build policy for the fork.
- Create a branch.
- Add a build policy for the master branch.
- Add an application access policy.
- Create a fork.

Answer Area

Answer:

Answer Area

- Create a repository
- Add a build policy for the master branch.
- Create a branch.

Question: 18

You need to implement Project4.
What should you do first?

A. Add the FROM instruction in the Dockerfile file.
B. Add a Copy and Publish Build Artifacts task to the build pipeline.
C. Add a Docker task to the build pipeline.
D. Add the MAINTAINER instruction in the Dockerfile file.

Answer: C

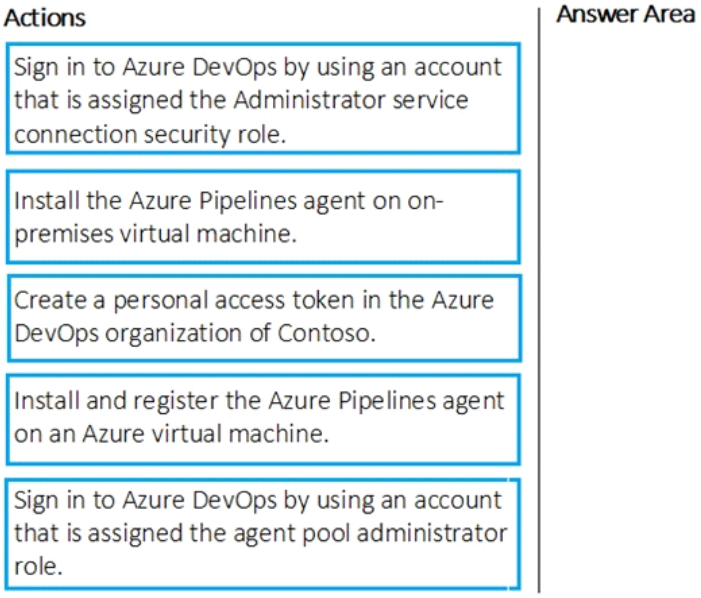
Explanation:
Scenario: Implement Project4 and configure the project to push Docker images to Azure Container Registry.

Project 4	Project4 will provide support for a build pipeline that creates a Docker image and pushes the image to the Azure Container Registry. Project4 will use an existing Dockerfile.

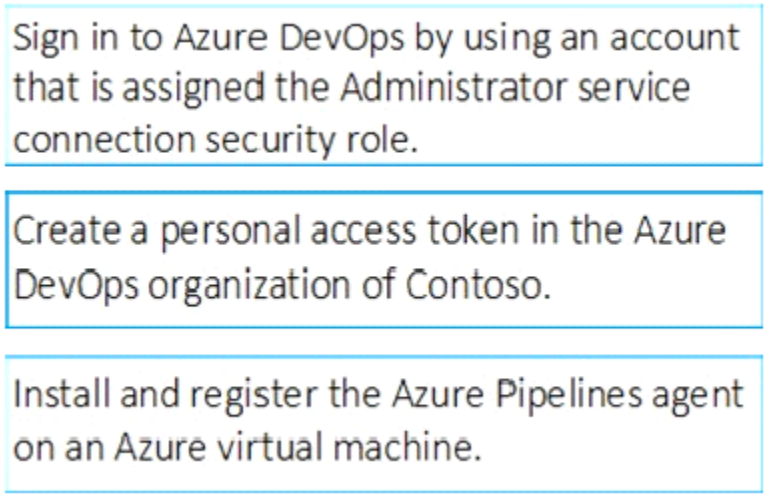
You use Azure Container Registry Tasks commands to quickly build, push, and run a Docker container image natively within Azure, showing how to offload your "inner-loop" development cycle to the cloud. ACR Tasks is a suite of features within Azure Container Registry to help you manage and modify container images across the container lifecycle.
References:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-quickstart-task-cli

Question: 19

You need to recommend a procedure to implement the build agent for Project1.
Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:
Scenario:

Project 1	Project1 will provide support for incremental builds and third-party SDK components

Step 1: Sign in to Azure Devops by using an account that is assigned the Administrator service connection security role.
Note: Under Agent Phase, click Deploy Service Fabric Application. Click Docker Settings and then click Configure Docker settings. In Registry Credentials Source, select Azure Resource Manager Service Connection. Then select your Azure subscription.
Step 2: Create a personal access token..
A personal access token or PAT is required so that a machine can join the pool created with the Agent Pools (read, manage) scope.
Step 3: Install and register the Azure Pipelines agent on an Azure virtual machine.
By running a Azure Pipeline agent in the cluster, we make it possible to test any service, regardless of type.
References:
https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-tutorial-deploy-container-app-with-cicd-vsts
https://mohitgoyal.co/2019/01/10/run-azure-devops-private-agents-in-kubernetes-clusters/
Topic 2, Mix Questions Set

Question: 20

Note: This question is part of a ser les 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 m this section, you will NOT be able to return to it As a result, these questions will not appear m the review screen
You integrate a cloud-hosted Jenkins server and a new Azure Dev Ops deployment.
You need Azure Dev Ops lo send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.
Solution: You create an email subscription to an Azure DevOps notification.
Does this meet the goal?

A. Yes
B. NO

Answer: B

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

Question: 21

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 m.ght 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 win NOT be able to return to it. As a result, these questions win 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

Question: 22

Note: This question part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the staled goals. Some question sets might have more than one correct solution, whale 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 depsoyment.
You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.
Solution: You add a trigger to the build pipeline.
Does this meet the goal?

A. Yes
B. NO

Answer: B

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

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 have an approval process that contains a condition. The condition requires that releases be approved by a team leader before they are deployed.
You haw a pokey stating that approvals must occur within eight hours.
You discover that deployments only if the approvals take longer than two hours.
You need to ensure that the deployments only fail if the approvals take longer than hours.
Solution From Post -deployment conditions, you modify the Timeout setting for post-deployment approvals.
Does this meet the goal?

A. Yes
B. NO

Answer: B

Question: 24

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 re-evaluation 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/en-us/azure/devops/pipelines/release/approvals/gates

Question: 25

Note: This question n 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 deployments fail if the approvals lake 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 Timeout setting for pre-deployment approvals.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Use a gate instead of an approval instead.
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates

Question: 26

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 prefect 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 select Enable continuous integration
Does the meet the goal?

A. Yes
B. No

Answer: A

References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/get-started-designer

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 ft. As a result these questions will not appear in the review screen.
You company has a prefect 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

Question: 28

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 project 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 Continuous deployment trigger settings of the release pipeline, you enable the Pull request trigger setting.
Does the meet the goal?

A. Yes
B. No

Answer: B

Explanation:
In Visual Designer you enable continuous integration (CI) by:
Select the Triggers tab.
Enable Continuous integration.
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/get-started-designer

Question: 29

You plan to create an image that will contain a .NET Core application.

You have a Dockerfile file that contains the following code. (Line numbers are included for reference only.)

```
01 FROM microsoft/dotnet:2.1-sdk
02 COPY ./
03 RUN dotnet publish -c Release -o out
04 FROM microsoft/dotnet:2.1-sdk
05 COPY -from=0 /out /
06 WORKDIR /
07 ENTRYPOINT ["dotnet", "appl.dll"]
```

You need to ensure that the image is as small as possible when the image is built.
Which line should you modify in the file?

A. 1
B. 3
C. 4
D. 7

Answer: C

Question: 30

Your company has a hybrid cloud between Azure and Azure Stack.
The company uses Azure DevOps for its CI/CD pipelines. Some applications are built by using Erlang and Hack.
You need to ensure that Erlang and Hack are supported as part of the build strategy across the hybrid cloud. The solution must minimize management overhead.
What should you use to execute the build pipeline?

A. AzureDevOps self-hosted agents on Azure DevTest Labs virtual machines.
B. AzureDevOps self-hosted agents on virtual machine that run on Azure Stack
C. AzureDevOps self-hosted agents on Hyper-V virtual machines
D. a Microsoft-hosted agent

Answer: B

Explanation:
Azure Stack offers virtual machines (VMs) as one type of an on-demand, scalable computing resource. You can choose a VM when you need more control over the computing environment.
References: https://docs.microsoft.com/en-us/azure/azure-stack/user/azure-stack-compute-overview

Question: 31

You are automating the build process for a Java-based application by using Azure DevOps.

You need to add code coverage testing and publish the outcomes to the pipeline.
What should you use?

A. Cobertura
B. Bullseye Coverage
C. MSTest
D. Coverlet

Answer: A

Explanation:
Use Publish Code Coverage Results task in a build pipeline to publish code coverage results to Azure Pipelines or TFS, which were produced by a build in Cobertura or JaCoCo format.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-code-coverage-results

Question: 32

You need to recommend a Docker container build strategy that meets the following requirements
• Minimizes image sues
• Minimizes the security surface area of the final image
What should you include m the recommendation?

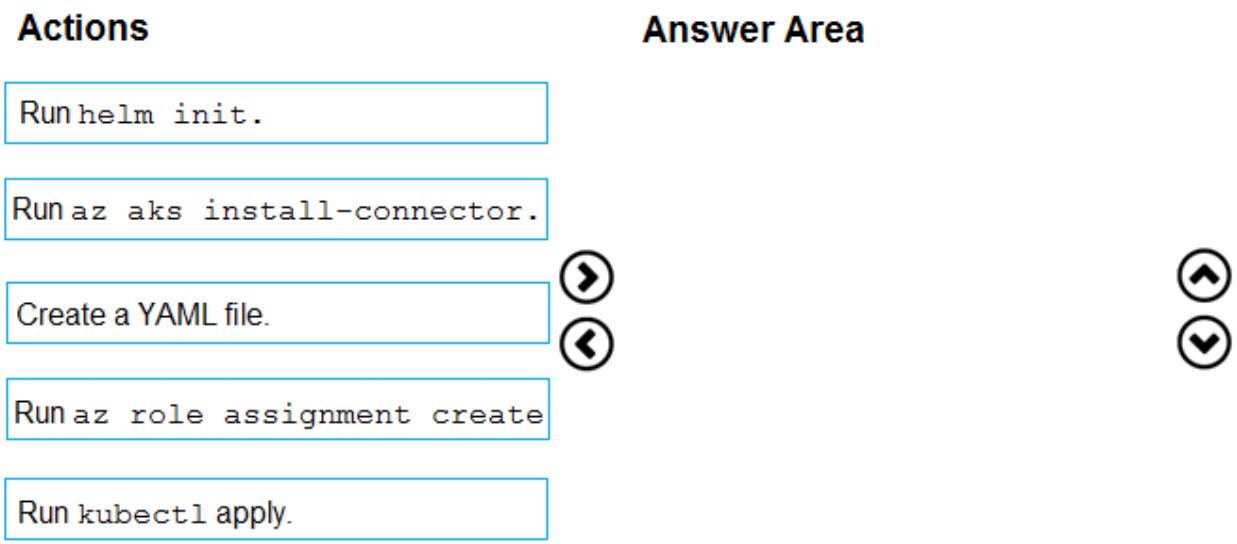
A. multi-stage builds
B. single-stage builds
C. PowerShell Desired State Configuration (DSC)
D. Docker Swarm

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/

Question: 33

You have an Azure Kubermets Service (AKS) implementation that is RBAC-enabled
You plan to use Azure Container Instances as a hosted development environment to run containers in the AKS implementation.
You need to conjure Azure Container Instances as a hosted environment for running me containers in AKS. Which three actions should you perform m sequence?
To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Create a YAML file.

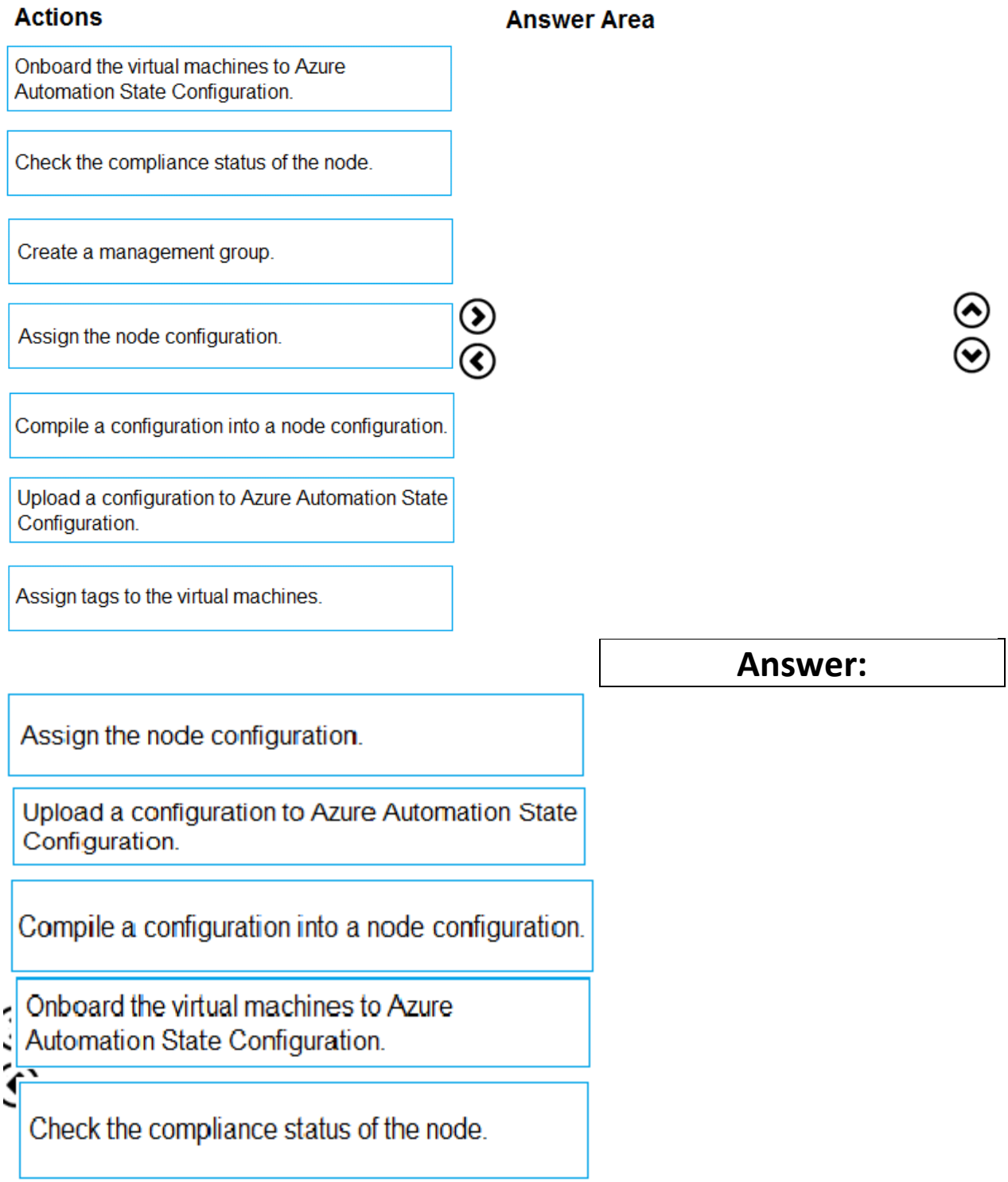
Run kubectl apply.

Run helm init.

Explanation:
Step 1: Create a YAML file.
If your AKS cluster is RBAC-enabled, you must create a service account and role binding for use with Tiller. To create a service account and role binding, create a file named rbac-virtual-kubelet.yaml
Step 2: Run kubectl apply.
Apply the service account and binding with kubectl apply and specify your rbac-virtual-kubelet.yaml file.
Step 3: Run helm init.
Configure Helm to use the tiller service account:
helm init --service-account tiller
You can now continue to installing the Virtual Kubelet into your AKS cluster.
References: https://docs.microsoft.com/en-us/azure/aks/virtual-kubelet

Question: 34

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.



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 — 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-dsc-getting-started

Question: 35

Your company builds a multi tier web application.
>You use Azure DevOps and host the production application on Azure virtual machines.
Your team prepares an Azure Resource Manager template of the virtual machine that you mil use to test new features.
You need to create a staging environment in Azure that meets the following requirements:
• Minimizes the cost of Azure hosting
• Provisions the virtual machines automatically
• Use* the custom Azure Resource Manager template to provision the virtual machines
What should you do?

A. In Azure DevOps, configure new tasks in the release pipeline to create and delete the virtual machines m Azure DevTest Labs.
B. From Azure Cloud Shell, run Azure PowerShell commands to create and delete the new virtual machines in a staging resource group.
C. In Azure DevOps, configure new tasks in the release pipeline to deploy to Azure Cloud Services.
D. In Azure Cloud Shell, run Azure CLI commands to create and delete the new virtual machines in a staging resource group.

Answer: A

Explanation:
You can use the Azure DevTest Labs Tasks extension that's installed in Azure DevOps to easily integrate your CI/CD build-and-release pipeline with Azure DevTest Labs. The extension installs three tasks:
Create a VM
Create a custom image from a VM
Delete a VM
The process makes it easy to, for example, quickly deploy a "golden image" for a specific test task and then delete it when the test is finished.
References: https://docs.microsoft.com/en-us/azure/lab-services/devtest-lab-integrate-ci-cd-vsts

Question: 36

You have a project Azure DevOps.
You plan to create a build pipeline that will deploy resources by using Azure Resource Manager templates. The templates will reference secretes stored in Azure Key Vault.
Yu 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 eh appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
"resources":[
{
  "apiversion": "2018-05-01",
  "name" : "secrets",
  "type":
```

- "Microsoft.KeyVault/vaults",
- "Microsoft.Resources/deployment".
- "Microsoft.Subscription/subscriptions".

```
  "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')]"
                }
               }
              }
             }
            }
          ],
```

Answer:

```
"resources":[
{
  "apiversion": "2018-05-01",
  "name" : "secrets",
  "type":
```

- "Microsoft.KeyVault/vaults",
- "Microsoft.Resources/deployment".
- "Microsoft.Subscription/subscriptions".

```
  "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')]"
            }
            }
           }
          }
         }
      ],
```

Question: 37

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

- A Key Vault access policy
- A Key Vault advanced access policy
- RBAC

Answer Area

Enable key vaults for template deployment by using: [ ]

Restrict access to the secrets in Key Vault by using: [ ]

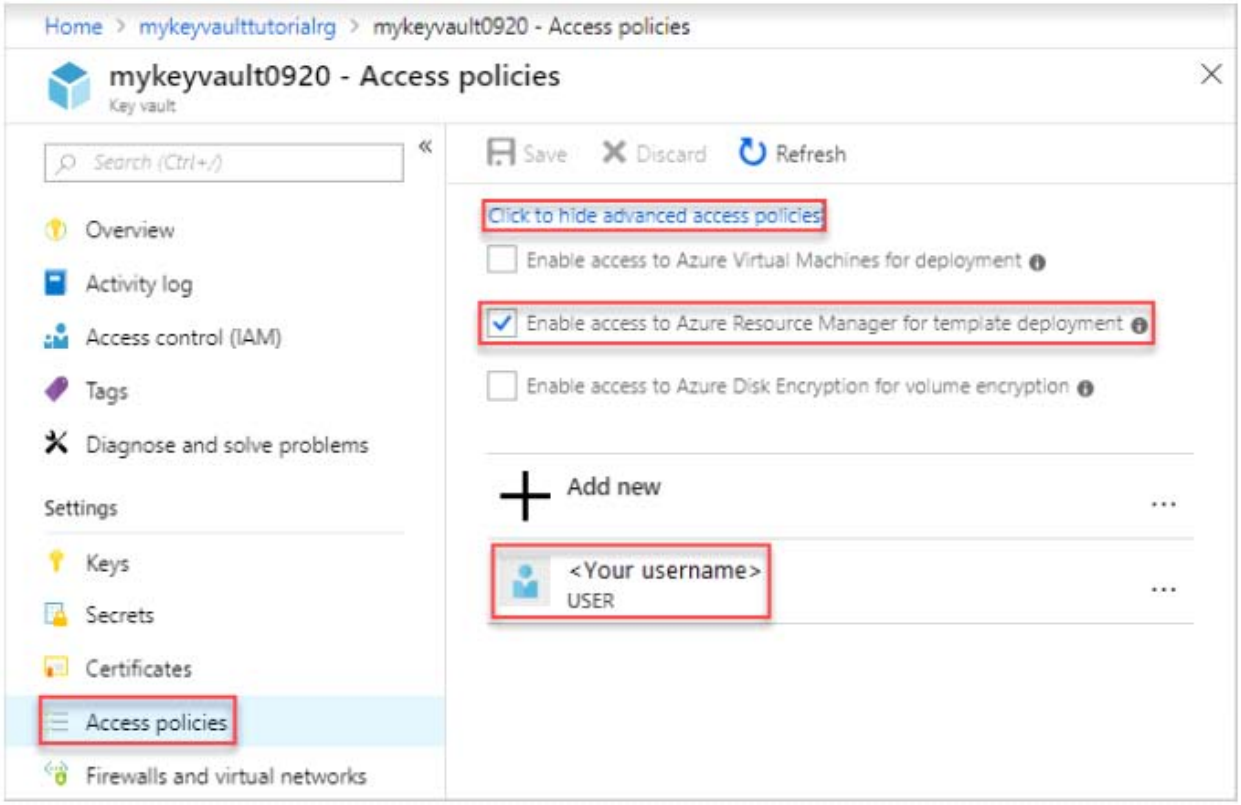
Answer:

Answer Area

Enable key vaults for template deployment by using: A Key Vault advanced access policy

Restrict access to the secrets in Key Vault by using: RBAC

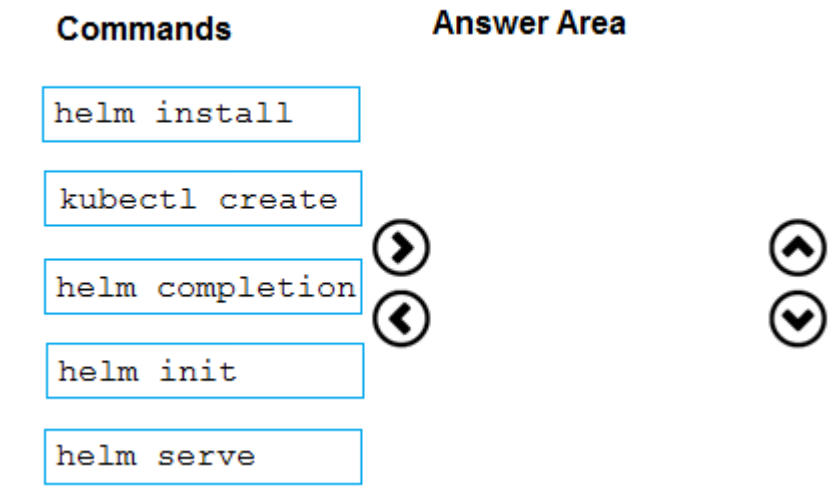
Explanation:
Box 1: A key Vault advanced access policy



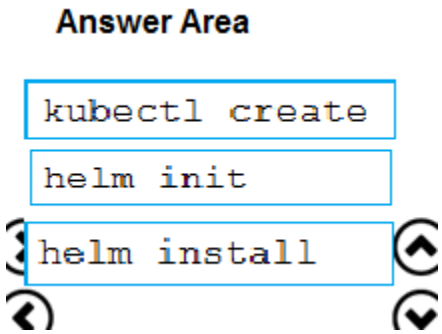
Box 2: RBAC
Management plane access control uses RBAC.
The management plane consists of operations that affect the key vault itself, such as:
Creating or deleting a key vault.
Getting a list of vaults in a subscription.
Retrieving Key Vault properties (such as SKU and tags).
Setting Key Vault access policies that control user and application access to keys and secrets.
References: https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-tutorial-use-key-vault

Question: 38

You need to recommend a solution for deploying charts by using Helm and Title to Azure Kubemets Service (AKS) in an RBAC-enabled cluster.
Which three commands should you recommend be run m sequence? To answer, move the appropriate commands from the list of commands to the answer area and arrange them in the correct order.



Answer:



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

Question: 39

You manage build pipelines and deployment pipelines by using Azure DevOps.
Your company has a team of 500 developers. New members are added continual lo the team
You need to automate me 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

References:
https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/migrate-to-group-based-resource-management?view=vsts&tabs=new-nav
https://docs.microsoft.com/en-us/rest/api/azure/devops/memberentitlementmanagement/?view=azure-devops-rest-5.0

Question: 40

During a code review, you discover many quality issues. Many modules contain unused variables and empty catch Modes. You need to recommend a solution to improve the quality o' 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 PMD.

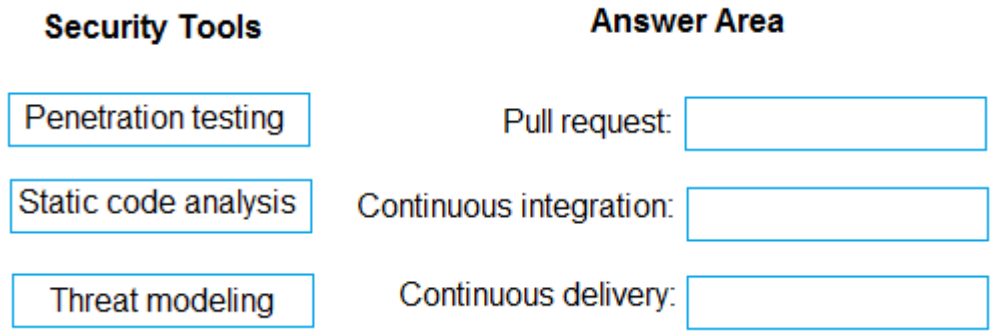
Answer: D

Explanation:

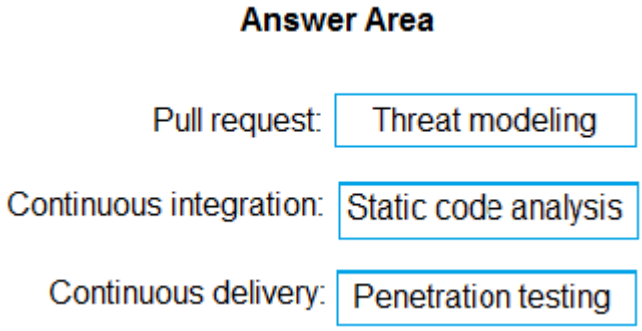
PMD is a source code analyzer. It finds common programming flaws like unused variables, empty catch blocks, unnecessary object creation, and so forth.
There is an Apache Maven PMD Plugin which allows you to automatically run the PMD code analysis tool on your project's source code and generate a site report with its results.
References: https://pmd.github.io/

Question: 41

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 toots 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.



Answer:



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/security-validation-cicd-pipeline?view=vsts

Question: 42

Your company plans to use an agile approach to software development
You need to recommend an application to provide communication between members of the development team who work in locations around the world. The application must meet the following requirements:
• Provide the ability to isolate the members of efferent project teams into separate communication channels and to keep a history of the chats within those channels.
• Be available on Windows 10, Mac OS, iOS, and Android operating systems.
• Provide the ability to add external contractors and suppliers to projects.
• Integrate directly with Azure DevOps.
What should you recommend?

A. Octopus
B. Bamboo
C. Microsoft Project
D. Slack

Answer: D

Explanation:
Slack is a popular team collaboration service that helps teams be more productive by keeping all communications in one place and easily searchable from virtually anywhere. All your messages, your files, and everything from Twitter, Dropbox, Google Docs, Azure DevOps, and more all together. Slack also has fully native apps for iOS and Android to give you the full functionality of Slack wherever you go.
Integrated with Azure DevOps
This integration keeps your team informed of activity happening in its Azure DevOps projects. With this integration, code check-ins, pull requests, work item updates, and build events show up directly in your team's Slack channel.
Note: Microsoft Teams would also be a correct answer, but it is not an option here.
References:
https://marketplace.visualstudio.com/items?itemName=ms-vsts.vss-services-slack

Question: 43

Your company uses Azure DevOps for the build pipelines and deployment pipelines of Java based projects. You need to recommend a strategy for managing technical debt.
Which two actions should you include in the recommendation? Each correct answer presents part of the solution
NOTE: Each correct selection is worth one point.

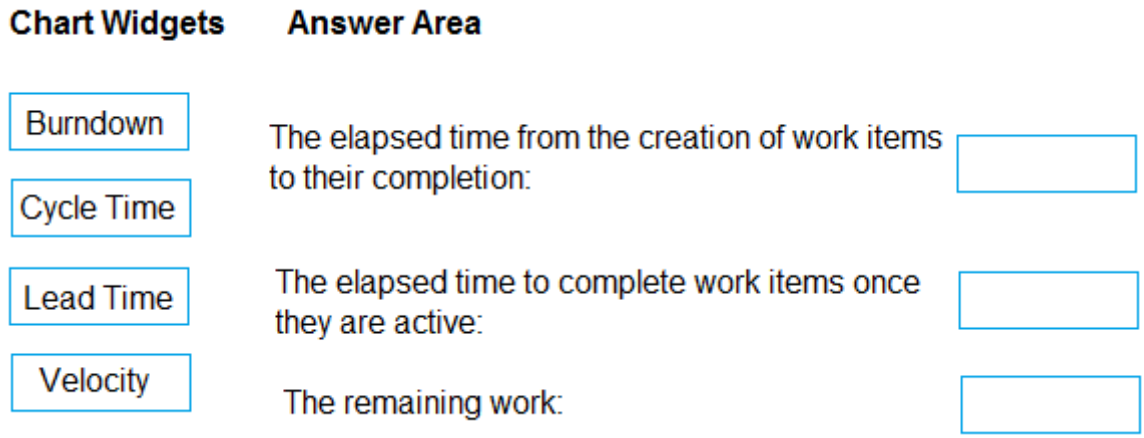
A. Integrate Azure DevOps and SonarQube.
B. Integrates Azure DevOPs and Azure DevTest Labs.
C. Configure post-deployment approvals in the deployment pipeline.

D. Configure pre-deployment approvals in the deployment pipeline.

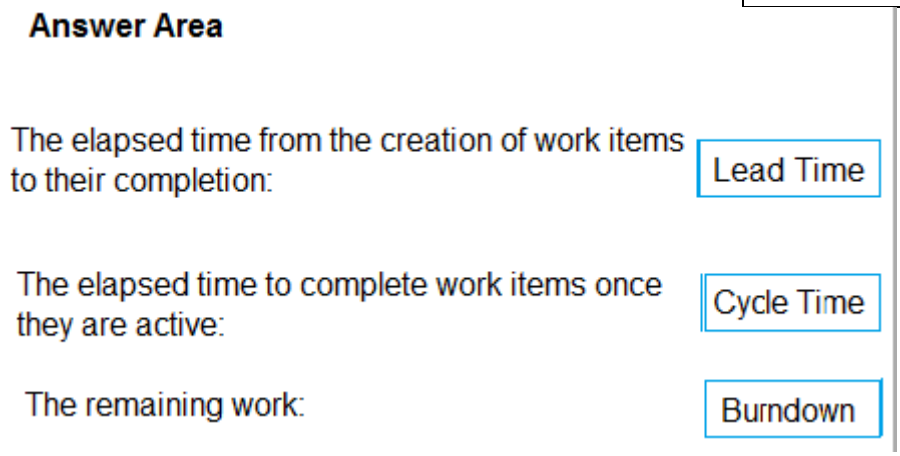
Answer: AC

Question: 44

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.



Answer:



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/velocity-guidance?view=vsts
https://docs.microsoft.com/en-us/azure/devops/report/dashboards/cycle-time-and-lead-time?view=vsts
https://docs.microsoft.com/en-us/azure/devops/report/dashboards/configure-burndown-burnup-widgets?view=vsts

Question: 45

Your company uses Team Foundation Server 2013 (TFS 2013).
You plan to migrate to Azure DevOps.
You need to recommend a migration strategy that meets the following requirements:
Preserves the dates of Team Foundation Version Control changesets
Preserves the changes dates of work items revisions
Minimizes migration effort
Migrates all TFS artifacts
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

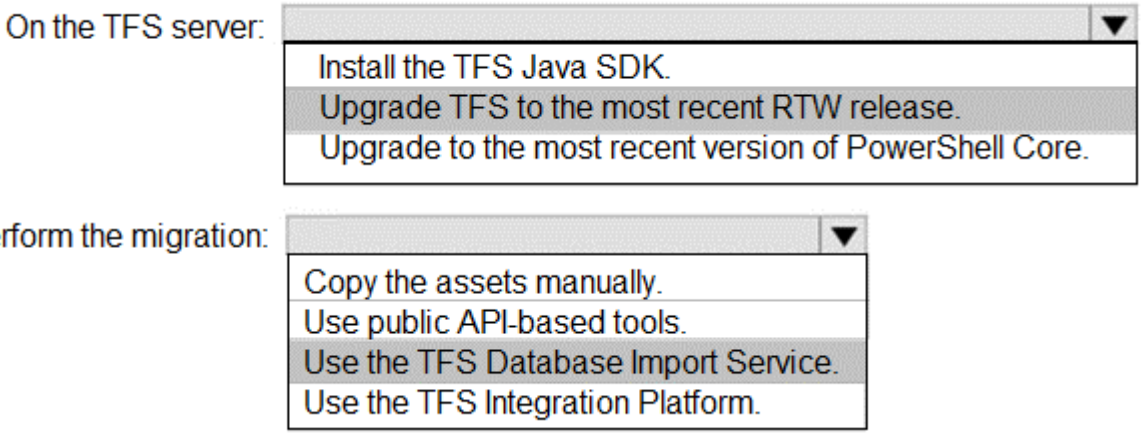
On the TFS server:

- Install the TFS Java SDK.
- Upgrade TFS to the most recent RTW release.
- Upgrade to the most recent version of PowerShell Core.

To perform the migration:

- Copy the assets manually.
- Use public API-based tools.
- Use the TFS Database Import Service.
- Use the TFS Integration Platform.

Answer:



Explanation:
Box 1: Upgrade TFS to the most recent RTM release.
One of the major prerequisites for migrating your Team Foundation Server database is to get your database schema version as close as possible to what is currently deployed in Azure Devops Services.
Box 2: Use the TFS Database Import Service
In Phase 3 of your migration project, you will work on upgrading your Team Foundation Server to one of the supported versions for the Database Import Service in Azure Devops Services.
References: Team Foundation Server to Azure Devops Services Migration Guide

Question: 46

Your company deploys applications m Docket containers.
You want to detect known exploits 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 exploits 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/security-validation-cicd-pipeline?view=vsts

Question: 47

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?

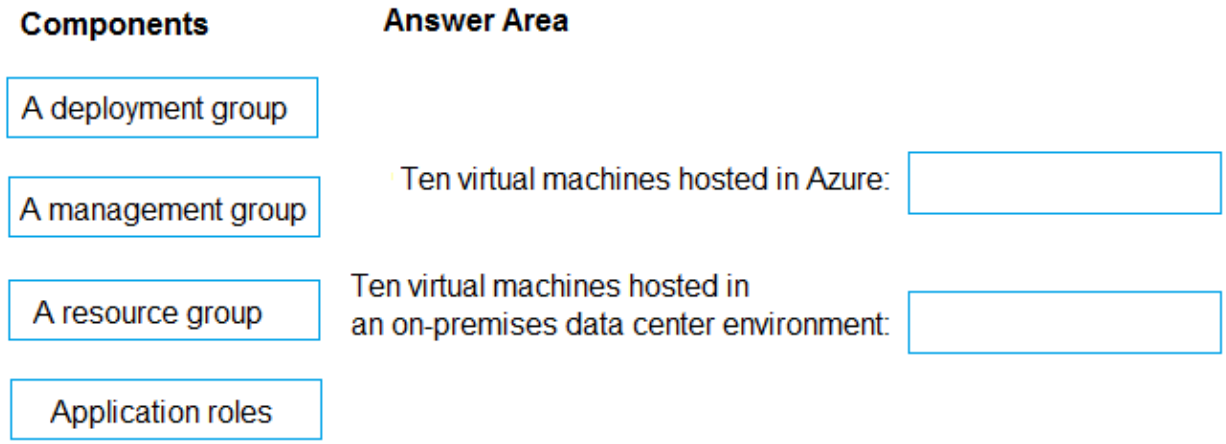
A. Service Map in Azure Log Analytics
B. Profiler in Azure Application Insights
C. availability tests in Azure Application Insights
D. Application Map in Azure Application Insights

Answer: C

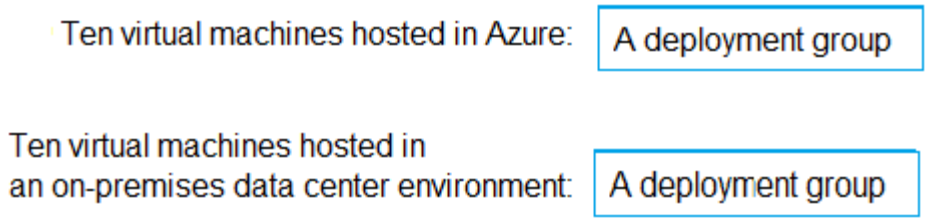
Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability

Question: 48

Your company plans to deploy an application to the following endpoints:
• Ten virtual machines hosted in Azure.
• Ten virtual machines hosted in an on-premises data center environment
All the virtual machines have the- Azure Pipelines agent.
You need to implement a release strategy for deploying the application to the endpoints.
What should you recommend using to deploy the application to the endpoints? To answer, drag the appropriate components to the correct endpoint.
Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or soon to view content
NOTE: Each correct selection n worth one point.



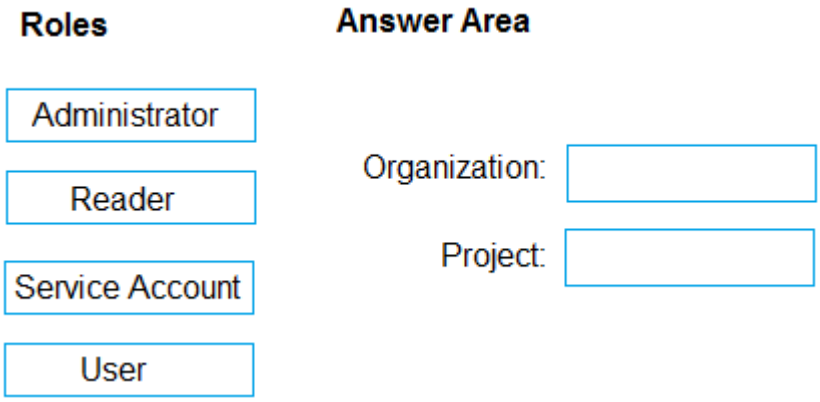
Answer:



Explanation:
Box 1: A deployment group
When authoring an Azure Pipelines or TFS Release pipeline, you can specify the deployment targets for a job using a deployment group.
If the target machines are Azure VMs, you can quickly and easily prepare them by installing the Azure Pipelines Agent Azure VM extension on each of the VMs, or by using the Azure Resource Group Deployment task in your release pipeline to create a deployment group dynamically.
Box 2: A deployment group
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deployment-groups

Question: 49

You need to configure access to Azure DevOps Agent pools to meet the forwarding requirements:
• Use a project agent pool when authoring build release pipelines.
• View the agent pool and agents of the organization.
• Use the principle of least privilege.
Which role memberships are required for the Azure 0e%Oos organization and the project? To answer, drag the appropriate role membership to the correct targets. Each role membership may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to content
NOTE: Each correct selection is worth one point.

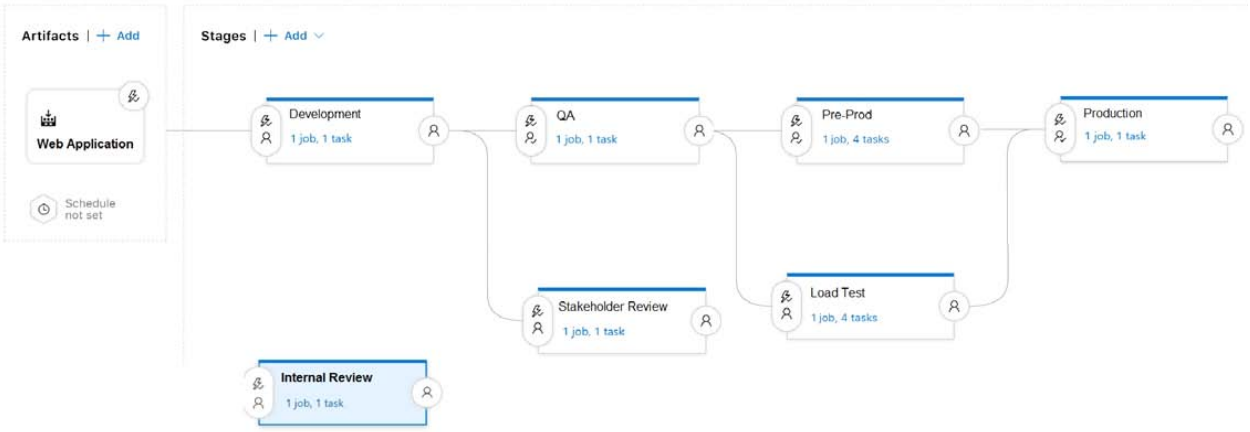


Answer:

project level role: User
Organization level role: Reader
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues

Question: 50

You are configuring a release pipeline in Azure DevOps as shown in the exhibit.



Use the drop-down menus to select the answer choice that answers each question based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

How many stages have triggers set?

- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7

Which component should you modify to enable continuous delivery?

- The Development stage
- The Internal Review stage
- The Production stage
- The Web Application artifact

Answer:

How many stages have triggers set?

- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7

Which component should you modify to enable continuous delivery?

- The Development stage
- The Internal Review stage
- The Production stage
- The Web Application artifact

Explanation:

Box 1: 5
There are five stages: Development, QA, Pre-production, Load Test and Production. They all have triggers.
Box 2: The Internal Review stage
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/triggers

Question: 51

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 stage.

Answer: AB

https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/servicenow?view=azure-devops

Question: 52

Your company has an on-premises Bitbucket Server that is used for Git-based source control. The server is protected by a firewall that blocks inbound Internet traffic.
You plan to use Azure DevOps to manage the build and release processes
Which two components are required to integrate Azure DevOps and Bitbucket?
Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one port.

A. an External Git service connection
B. a Microsoft hosted agent
C. service hooks
D. a self- hosted agent
E. a deployment M group

Answer: AD

When a pipeline uses a remote, 3rd-party repository host such as Bitbucket Cloud, the repository is configured with webhooks that notify Azure Pipelines Server or TFS when code has changed and a build should be triggered. Since on-premises installations are normally protected behind a firewall, 3rd-party

webhooks are unable to reach the on-premises server. As a workaround, you can use the External Git repository type which uses polling instead of webhooks to trigger a build when code has changed.
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/pipeline-options-for

Question: 53

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: • 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

- Git
- Perforce
- Subversion
- Team Foundation Version Control

Answer Area

- Project 1:
- Project 2:
- Project 3:
- Project 4:

Answer:

Answer Area

Project 1:	Team Foundation Version Control
Project 2:	Git
Project 3:	Subversion
Project 4:	Git

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-git-xcode
https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/overview

Question: 54

You mc configuring Azure DevOps build pipelines.
You plan to use hosted build agents.
Which build agent pool should you use to compile each application type? To answer, drag the appropriate built agent pools to the correct application types. Each butt agent pool 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.

Build Agent Pools

- Hosted Windows Container
- Hosted Ubuntu 1604
- Hosted macOS
- Hosted
- Default

Answer Area

An application that runs on iOS: _____

An Internet Information Services (IIS) web application that runs in Docker: _____

Answer:

An application that runs on iOS: Hosted macOS

An Internet Information Services (IIS) web application that runs in Docker: Hosted

Explanation:
Box 1: Hosted macOS
Hosted macOS pool (Azure Pipelines only): Enables you to build and release on macOS without having to configure a self-hosted macOS agent. This option affects where your data is stored.
Box 2: Hosted
Hosted pool (Azure Pipelines only): The Hosted pool is the built-in pool that is a collection of Microsoft-hosted agents.
Incorrect Answers:
Default pool: Use it to register self-hosted agents that you've set up.
Hosted Windows Container pool (Azure Pipelines only): Enabled you to build and release inside Windows containers. Unless you're building using containers, Windows builds should run in the Hosted VS2017 or Hosted pools.
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-osx

Question: 55

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 tor 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 the with other Git permissions.
References: https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

Question: 56

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?

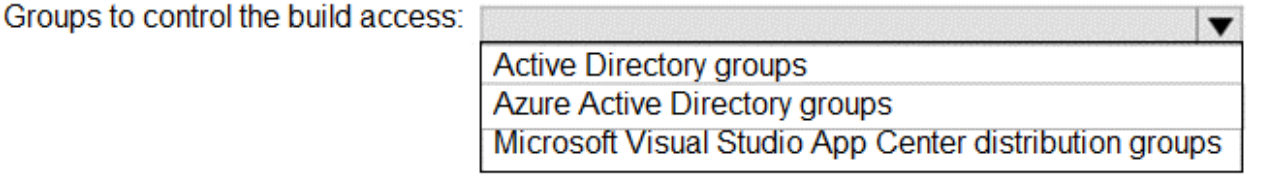
A. an Azure Resource Manager parameter file
B. an Azure Storage table
C. an Appsettings.json files
D. Azure Key Vault
E. a Web.config file

Answer: D

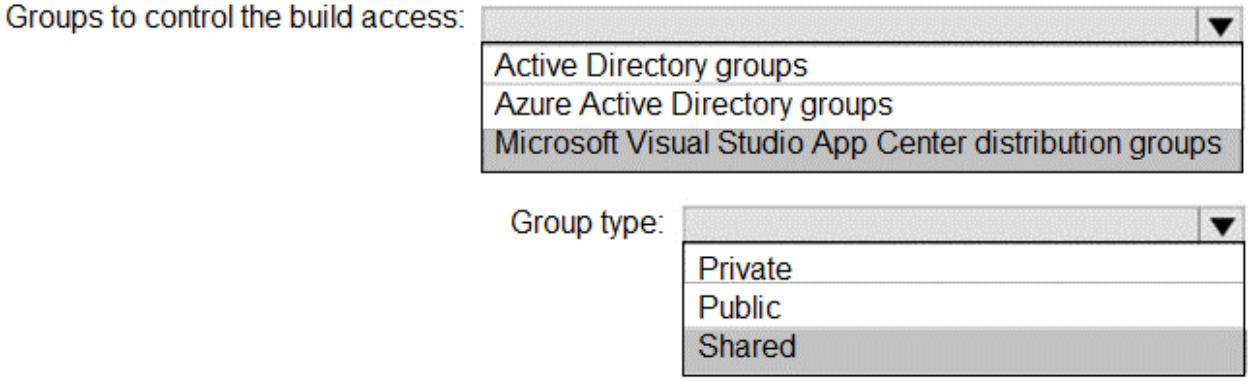
Explanation:
When you need to pass a secure value (like a password) as a parameter during deployment, you can retrieve the value from an Azure Key Vault. You retrieve the value by referencing the key vault and secret in your parameter file. The value is never exposed because you only reference its key 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: 57

Your company is creating a suite of three mobile applications.
You need to control access to the application builds. The solution must be managed at the organization level
What should you use? To answer, select the appropriate options m the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
Box 1: Microsoft Visual Studio App Center distribution Groups
Distribution Groups are used to control access to releases. A Distribution Group represents a set of users that can be managed jointly and can have common access to releases. Example of Distribution Groups can be teams of users, like the QA Team or External Beta Testers or can represent stages or rings of releases, such as Staging.
Box 2: Shared
Shared distribution groups are private or public distribution groups that are shared across multiple apps in a single organization. Shared distribution groups eliminate the need to replicate distribution groups across multiple apps.
Note: With the Deploy with App Center Task in Visual Studio Team Services, you can deploy your apps from Azure DevOps (formerly known as VSTS) to App Center. By deploying to App Center, you will be able to distribute your builds to your users.
References: https://docs.microsoft.com/en-us/appcenter/distribution/groups

Question: 58

Your company uses a Git repository in Azure Repos lo 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 tingle 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-with-squash

Question: 59

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 m your Azure DevOps account.
C. Create a webhook in Jenkins.
D. Add a domain to your Jenkins account.
E. Create a service hook m Azure DevOps.

Answer: ABE

References:
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: 60

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: C

https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/github?view=azure-devops&tabs=yaml

Question: 61

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 build
References: https://docs.microsoft.com/en-us/azure/devops/artifacts/concepts/upstream-sources?view=vsts

Question: 62

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/feed-permissions?view=vsts&tabs=new-nav

Question: 63

Your company « 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

Question: 64

You 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: D

Explanation:
Separate Your Dependencies
Within 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: 65

You use Azure SQL Database Intelligent Insights and Azure Application Insights foe 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

Question: 66

Your 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?

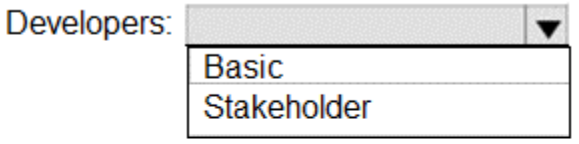
A. Automation & Control
B. IT Service Management Connector (ITSM)
C. Application lmiQ.hu Connector
D. insight & Analytics

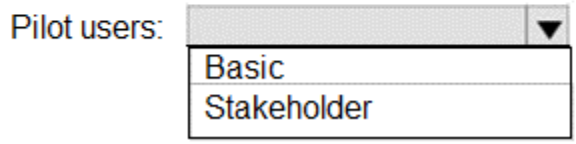
Answer: B

Explanation:
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:
ServiceNow
System Center Service Manager
Provance
Cherwell
With ITSMC, you can
Create 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

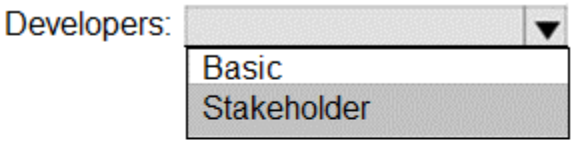
Question: 67

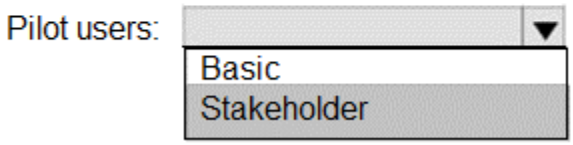
Your company is building a new web application.
You plan to collect feedback from pilot users on the features being delivered.
All the pilot users have a corporate computer that has Google Chrome and the Microsoft Test & Feedback extension installed. The pilot users will test the application by using Chrome.
You need to identify which access levels are required to ensure that developers can request and gather feedback from the pilot users. The solution must use the principle of least privilege.
Which access levels m Azure DevOps should you identify? To answer, select the appropriate options in the answer area
NOTE: Each correct selection is worth one point.





Answer:





Explanation:
Box 1: Basic
Assign Basic to users with a TFS CAL, with a Visual Studio Professional subscription, and to users for whom you are paying for Azure Boards & Repos in an organization.
Box 2: Stakeholder
Assign Stakeholders to users with no license or subscriptions who need access to a limited set of features.
Note:
You assign users or groups of users to one of the following access levels:
Basic: provides access to most features
VS Enterprise: provides access to premium features
Stakeholders: provides partial access, can be assigned to unlimited users for free
References: https://docs.microsoft.com/en-us/azure/devops/organizations/security/access-levels?view=vsts

Question: 68

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

C. Azure Event Hubs
D. 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/collect-azurepass-posh

Question: 69

Your company creates a web application.
You need to recommend a solution that automatically sends to Microsoft Teams a dairy summary of the exceptions that occur m the application.
Which two Azure services should you recommend? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Visual Studio App Center
B. Azure DevOps Project
C. Azure Logic Apps
D. Azure Pipelines
E. Azure Application Insights

Answer: CE

References:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/asp-net-exceptions
https://docs.microsoft.com/en-us/azure/azure-monitor/app/automate-custom-reports

Question: 70

Your company plans to use an agile approach to software development.
You need to recommend an application to provide communication between members of the development team who work in locations around the world. The applications must meet the following requirements:
Provide the ability to isolate the members of different project teams into separate communication channels and to keep a history of the chats within those channels.
Be available on Windows 10, Mac OS, iOS, and Android operating systems.
Provide the ability to add external contractors and suppliers to projects.
Integrate directly with Azure DevOps.
What should you recommend?

A. Microsoft Project
B. Bamboo
C. Microsoft Lync
D. Microsoft Teams

Answer: D

Explanation:
Within each team, users can create different channels to organize their communications by topic. Each channel can include a couple of users or scale to thousands of users.
Microsoft Teams works on Android, iOS, Mac and Windows systems and devices. It also works in Chrome, Firefox, Internet Explorer 11 and Microsoft Edge web browsers.
The guest-access feature in Microsoft Teams allows users to invite people outside their organizations to join internal channels for messaging, meetings and file sharing. This capability helps to facilitate business-to-business project management.
Teams integrates with Azure DevOps.
References: https://searchunifiedcommunications.techtarget.com/definition/Microsoft-Teams

Question: 71

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 project 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 Pre-deployment conditions settings of the release pipeline, you select After stage.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead, In Visual Designer you enable continuous integration (CI) by:
Select the Triggers tab.
Enable Continuous integration.
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/get-started-designer

Question: 72

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 project 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 Pre-deployment conditions settings of the release pipeline, you select Batch changes while a build is in progress.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Use a Pull request trigger.
Note: Batch changes
Select this check box if you have a lot of team members uploading changes often and you want to reduce the number of builds you are running. If you select this option, when a build is running, the system waits until the build is completed and then queues another build of all changes that have not yet been built.
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/build/triggers

Question: 73

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 re-evaluation of gates option.
Does this meet the goal?

A. Yes
B. No

Answer: B

References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates

Question: 74

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:
Two resource groups
Four Azure virtual machines in one resource group
Two Azure SQL databases in other resource group
You need to recommend a solution to deploy the resources.
Solution: Create two standalone templates, each of which will deploy the resources in its respective group.
Does this meet the goal?

A. Yes
B. No

Answer: A

References: https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-linked-templates

Question: 75

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:
Two resource groups
Four Azure virtual machines in one resource group
Two 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-resource-manager/resource-group-linked-templates

Question: 76

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:
Two resource groups
Four Azure virtual machines in one resource group
Two Azure SQL databases in other resource group
You need to recommend a solution to deploy the resources.
Solution: Create a main template that has two linked templates, each of which will deploy the resource in its respective group.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
To deploy your solution, you can use either a single template or a main template with many related templates. The related template can be either a separate file that is linked to from the main template, or a template that is nested within the main template.
References: https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-linked-templates

Question: 77

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:
Detect and remedy vulnerable open source components.
Generate comprehensive open source inventory reports per project or build.
Enforce open source license compliance, including dependencies' licenses.
Identify outdated open source libraries with recommendations to update.
References: https://www.azuredevopslabs.com/labs/vstsextend/WhiteSource/

Question: 78

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 build completed event
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
You can create a service hook for Azure DevOps Services and TFS with Jenkins.
However, the service subscription event should use the code pushed event, is triggered when the code is pushed to a Git repository.

Question: 79

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

Explanation:
A successful IOS device build will produce an ipa file. In order to install the build on a device, it needs to be signed with a valid provisioning profile and certificate. To sign the builds produced from a branch, enable code signing in the configuration pane and upload a provisioning profile (.mobileprovision) and a valid certificate (.p12), along with the password for the certificate.
References:
https://docs.microsoft.com/en-us/appcenter/build/xamarin/ios/

Question: 80

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

Question: 81

Your company is building a mobile app that targets Android devices and OS devices. Your team uses Azure DevOps to manage all work items and release cycles. You need to recommend a solution to perform the following tasks:
- Collect crash reports for issue analysis
- Distribute beta releases to your testers.
- Get user feedback on the functionality of new apps.

What should you include in the recommendation?

A. Jenkins integration

B. Azure Application Insights widgets
C. the Microsoft Test & Feedback extension
D. Microsoft Visual Studio App Center integration

Answer: C

Explanation:
The "Exploratory Testing" extension is now "Test & Feedback" and is now Generally Available.
Anyone can now test web apps and give feedback, all directly from the browser on any platform: Windows, Mac, or Linux. Available for Google Chrome and Mozilla Firefox (required version 50.0 or above) currently. Support for Microsoft Edge is in the pipeline and will be enabled once Edge moves to a Chromium-compatible web platform.
References:
https://marketplace.visualstudio.com/items?itemName=ms.vss-exploratorytesting-web

Question: 82

Your company is building a new solution in Java.
The company currently uses a SonarQube server to analyze the code of .NET solutions.
You need to analyze and monitor the code quality of the Java solution.
Which task types should you add to the build pipeline?

A. Octopus
B. Chef
C. Maven
D. Grunt

Answer: A

Question: 83

Your company has a project in Azure DevOps.
You need to ensure that when there are multiple builds pending deployment only the most recent build is deployed.
What should you use?

A. deployment queue settings
B. deployment conditions
C. release gates
D. pull request triggers

Answer: A

References:

https://docs.microsoft.com/en-us/azure/devops/pipelines/process/stages?tabs=classic&view=azure-devops#queuing-policies

Question: 84

Your company develops a client banking application that processes a large volume of data.
Code quality is an ongoing issue for the company. Recently, the code quality has deteriorated because of an increase in time pressure on the development team.
You need to implement static code analysis.
During which phase should you use static code analysis?

A. build
B. production release
C. staging
D. integration testing

Answer: D

Explanation:
The Secure Development Lifecycle (SDL) Guidelines recommend that teams perform static analysis during the implementation phase of their development cycle.
Note: The company should focus in particular on the implementation of DevOps tests to assess the quality of the software from the planning stage to the implementation phase of the project.
References:
https://secdevtools.azurewebsites.net/

Question: 85

You have a GitHub repository.
You create a new repository in Azure DevOps.
You need to recommend a procedure to clone the repository from GitHub to Azure DevOps.
What should you recommend?

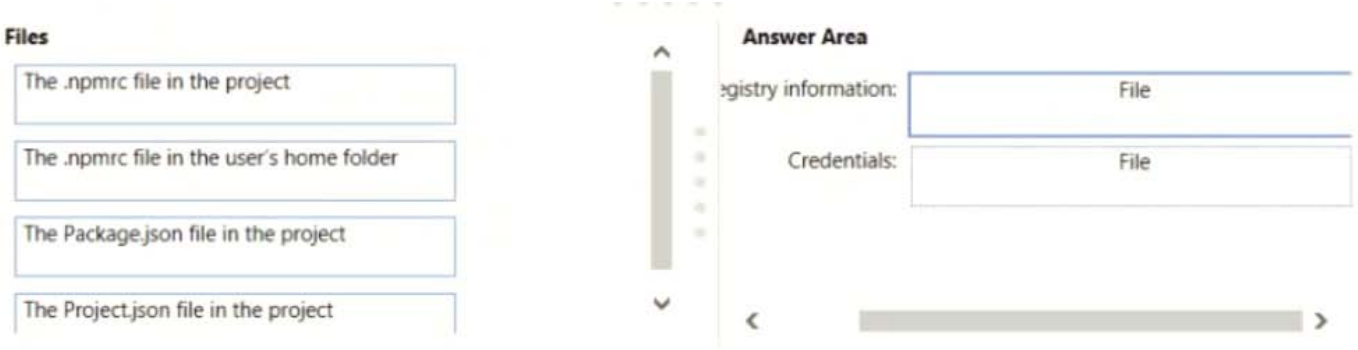
A. Create a webhook.
B. Create a service connection for GitHub.
C. From Import a Git repository, click Import
D. Create a pull request.
E. Create a personal access token in Azure DevOps.

Answer: C

Question: 86

You are implementing a package management solution for a Node.js application by using Azure Artifacts.
You need to configure the development environment to connect to the package repository. The solution must minimize the likelihood that credentials will be leaked.
Which file should you use to configure each connection? To answer, drag the appropriate files to the correct connections. Each file 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.



Answer:

Feed registry information: The .npmrc file in the project

Credentials: The npmrc file in the user's home folder

Explanation:
All Azure Artifacts feeds require authentication, so you'll need to store credentials for the feed before you can install or publish packages. npm uses .npmrc configuration files to store feed URLs and credentials. Azure DevOps Services recommends using two .npmrc files.
Feed registry information: The .npmrc file in the project
One .npmrc should live at the root of your git repo adjacent to your project's package.json. It should contain a "registry" line for your feed and it should not contain credentials since it will be checked into git.
Credentials: The .npmrc file in the user's home folder
On your development machine, you will also have a .npmrc in $home for Linux or Mac systems or $env.HOME for win systems. This .npmrc should contain credentials for all of the registries that you need to connect to. The NPM client will look at your project's .npmrc, discover the registry, and fetch matching credentials from $home/.npmrc or $env.HOME/.npmrc.
References:
https://docs.microsoft.com/en-us/azure/devops/artifacts/npm/npmrc?view=azure-devops&tabs=windows

Question: 87

Your company is concerned that when developers introduce open source libraries, it creates licensing compliance issues.

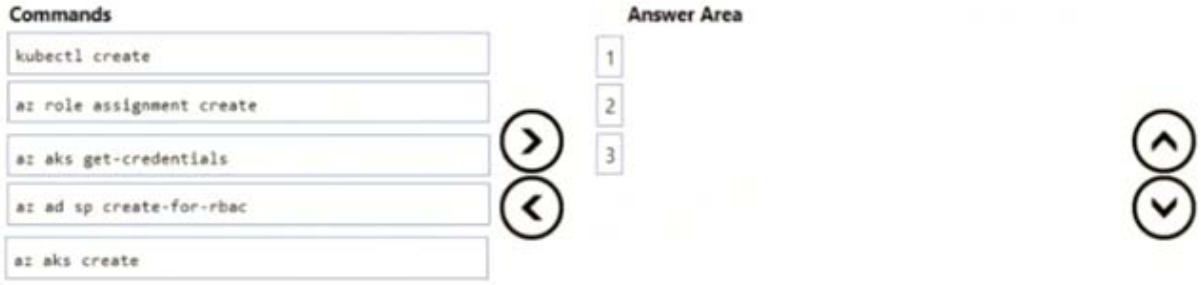
You need to add an automated process to the build pipeline to detect when common open source libraries are added to the code base.
What should you use?

A. PDM
B. OWASPZAP
C. WhiteSource
D. Jenkins

Answer: C

Question: 88

You plan to use Azure Kubernetes Service (AKS) to host containers deployed from images hosted in a Docker Trusted Registry.
You need to recommend a solution for provisioning and connecting to AKS. The solution must ensure that AKS is RBAC-enaWed and uses a custom service principal.
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 coned order.



Answer:

az aks create

az ad sp create-for-rbac

kubectl create

Explanation:
Step 1 : az acr create
An Azure Container Registry (ACR) can also be created using the new Azure CLI.
az acr create
--name <REGISTRY_NAME>
--resource-group <RESOURCE_GROUP_NAME>
--sku Basic

Step 2: az ad sp create-for-rbac
Once the ACR has been provisioned, you can either enable administrative access (which is okay for testing) or you create a Service Principal (sp) which will provide a client_id and a client_secret.
az ad sp create-for-rbac
--scopes
/subscriptions/<SUBSCRIPTION_ID>/resourcegroups/<RG_NAME>/providers/Microsoft.ContainerRegistry/registries/<REGISTRY_NAME>
--role Contributor
--name <SERVICE_PRINCIPAL_NAME>
Step 3: kubectl create
Create a new Kubernetes Secret.
kubectl create secret docker-registry <SECRET_NAME>
--docker-server <REGISTRY_NAME>.azurecr.io
--docker-email <YOUR_MAIL>
--docker-username=<SERVICE_PRINCIPAL_ID>
--docker-password <YOUR_PASSWORD>
References:
https://thorsten-hans.com/how-to-use-private-azure-container-registry-with-kubernetes

Question: 89

Your company has a project in Azure DevOps for a new application. The application will be deployed to several Azure virtual machines that run Windows Server 2016.
You need to recommend a deployment strategy for the virtual machines. The strategy must meet the following requirements:
- Ensure that the virtual machines maintain a consistent configuration.
- Minimize administrative effort to configure the virtual machines

What should you include in the recommendation?

A. Deployment YAML and Azure pipeline stage templates
B. Azure Resource Manager templates and the Custom Script Extension for Windows
C. Azure Resource Manager templates and the PowerShell Desired State Configuration (DSC) extension for Windows
D. Deployment YAML and Azure pipeline deployment groups

Answer: B

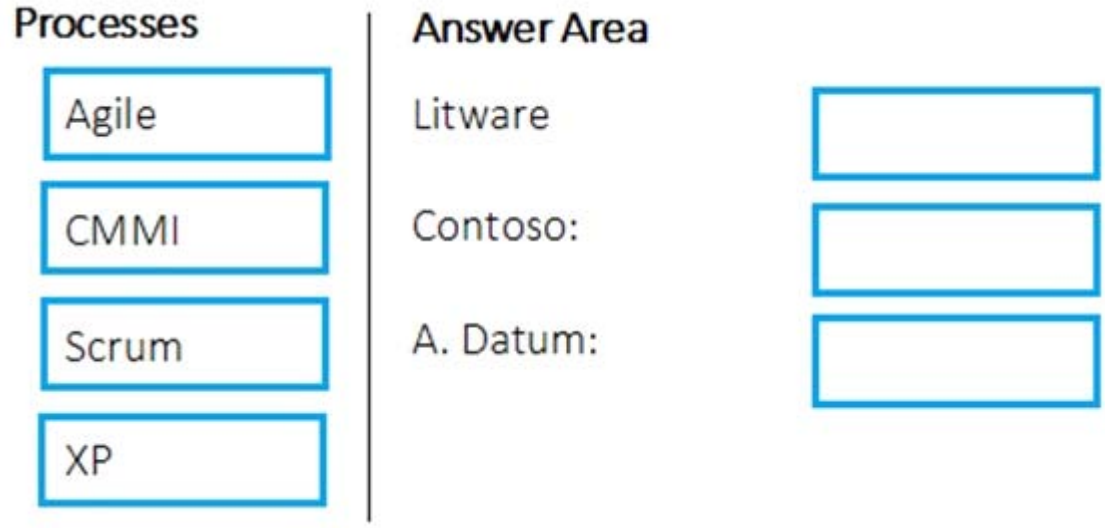
Explanation:
The Custom Script Extension downloads and executes scripts on Azure virtual machines. This extension is useful for post deployment configuration, software installation, or any other configuration or management tasks. Scripts can be downloaded from Azure storage or GitHub, or provided to the Azure portal at extension run time. The Custom Script Extension integrates with Azure Resource Manager templates, and can be run using the Azure CLI, PowerShell, Azure portal, or the Azure Virtual Machine REST API.
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/custom-script-windows

Question: 90

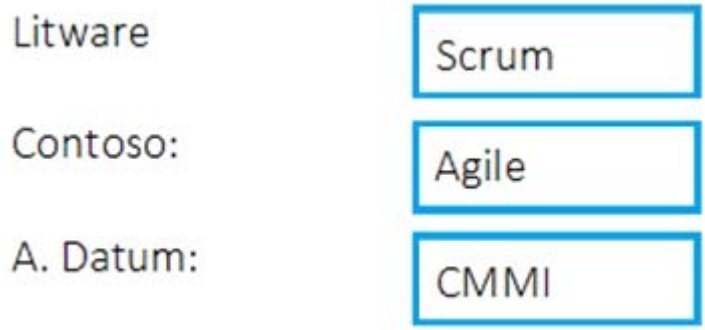
You are planning projects for three customers. Each customer's preferred process for work items is shown in the following table.

Customer name	Preferred process
Litware, Inc.	Track product backlog items (PBIs) and bugs on the Kanban board. Break the PBIs down into tasks on the task board.
Contoso, Ltd.	Track user stories and bugs on the Kanban board. Track the bugs and tasks on the task board.
A. Datum Corporation	Track requirements, change requests, risks, and reviews.

The customers all plan to use Azure DevOps for work item management.
Which work item process should you use for each customer? To answer, drag the appropriate work item process to the correct customers. Each work item process 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.



Answer:



Explanation:
Box 1: Scrum
Choose Scrum when your team practices Scrum. This process works great if you want to track product backlog items (PBIs) and bugs on the Kanban board, or break PBIs and bugs down into tasks on the taskboard.
Box 2: Agile
Choose Agile when your team uses Agile planning methods, including Scrum, and tracks development and test activities separately. This process works great if you want to track user stories and (optionally) bugs on the Kanban board, or track bugs and tasks on the taskboard.
Box 3: CMMI
Choose CMMI when your team follows more formal project methods that require a framework for process improvement and an auditable record of decisions. With this process, you can track requirements, change requests, risks, and reviews.
Incorrect Answers:
XP:
The work tracking objects contained within the default DevOps processes and DevOps process templates are Basic, Agile, CMMI, and Scrum
XP (Extreme Programming) and DevOps are different things. They don't contradict with each other, they can be used together, but they have different base concepts inside them.
References:
https://docs.microsoft.com/en-us/azure/devops/boards/work-items/guidance/choose-process?view=azure-devops

Question: 91

Your development team is building a new web solution by using the Microsoft Visual Studio integrated development environment (IDE).
You need to make a custom package available to all the developers. The package must be managed centrally,
and the latest version must be available for consumption in Visual Studio automatically.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Publish the package to a feed.
B. Create a new feed in Azure Artifacts.
C. Upload a package to a Git repository.
D. Add the package URL to the Environment settings in Visual Studio.
E. Add the package URL to the NuGet Package Manager settings in Visual Studio.
F. Create a Git repository in Azure Repos.

Answer: ABE

Explanation:
B: By using your custom NuGet package feed within your Azure DevOps (previously VSTS) instance, you'll be
able to distribute your packages within your organization with ease.
Start by creating a new feed.
A: We can publish, pack and push the built project to our NuGet feed.

E: Consume your private NuGet Feed
Go back to the Packages area in Azure DevOps, select your feed and hit “Connect to feed”. You’ll see some
instructions for your feed, but it’s fairly simple to set up.
Just copy your package source URL, go to Visual Studio, open the NuGet Package Manager, go to its settings
and add a new source. Choose a fancy name, insert the source URL. Done.
Search for your package in the NuGet Package Manager and it should appear there, ready for installation.
Make sure to select the appropriate feed (or just all feeds) from the top right select box.
References:
https://medium.com/medialesson/get-started-with-private-nuget-feeds-in-azure-devops-8c7b5f022a68

Question: 92

Your company uses Azure DevOps.
Only users who have accounts in Azure Active Directory can access the Azure DevOps environment.
You need to ensure that only devices that are connected to the on-premises network can access the Azure
DevOps environment.
What should you do?

A. Assign the Stakeholder access level all users.
B. In Azure Active Directory, configure risky sign-ins.
C. In Azure DevOps, configure Security in Project Settings.
D. In Azure Active Directory, configure conditional access.

Answer: D

Explanation:
Conditional Access is a capability of Azure Active Directory. With Conditional Access, you can implement automated access control decisions for accessing your cloud apps that are based on conditions.
Conditional Access policies are enforced after the first-factor authentication has been completed.
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Question: 93

You are automating the testing process for your company.
You need to automate UI testing of a web application.
Which framework should you use?

A. JaCoco
B. Selenium
C. Xamarin.UITest
D. Microsoft.CodeAnalysis

Answer: B

Explanation:
Performing user interface (UI) testing as part of the release pipeline is a great way of detecting unexpected changes, and need not be difficult. Selenium can be used to test your website during a continuous deployment release and test automation.
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/test/continuous-test-selenium?view=azure-devops

Question: 94

You have an Azure DevOps organization named Contoso, an Azure DevOps project named Project1, an Azure subscription named Sub1, and an Azure key vault named vault1.
You need to ensure that you can reference the values of the secrets stored in vault1 in all the pipelines of
Project1. The solution must prevent the values from being stored in the pipelines.
What should you do?

A. Create a variable group in Project1.
B. Add a secure file to Project1.
C. Modify the security settings of the pipelines.
D. Configure the security policy of Contoso.

Answer: A

Explanation:
Use a variable group to store values that you want to control and make available across multiple pipelines.
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/library/variable-groups

Question: 95

You are configuring Azure Pipelines for three projects in Azure DevOps as shown in the following table.

Project name	Project Details
Project1	The project team provides preconfigured YAML files that it wants to use to manage future pipeline configuration changes.
Project2	The sensitivity of the project requires that the source code be hosted on the managed Windows server on your company's network.
Project3	The project team requires a centralized version control system to ensure that developers work with the most recent version.

Which version control system should you recommend 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

- Assembla Subversion
- Bitbucket Cloud
- Git in Azure Repos
- GitHub Enterprise

Answer Area

Project1: [ ]

Project2: [ ]

Project3: [ ]

Answer:

Project1: Git in Azure Repos

Project2: GitHub Enterprise

Project3: Bitbucket Cloud

Explanation:
Project1:Git in Azure Repos
Project2: Github Enterprise

GitHub Enterprise is the on-premises version of GitHub.com. GitHub Enterprise includes the same great set of features as GitHub.com but packaged for running on your organization's local network. All repository data is stored on machines that you control, and access is integrated with your organization's authentication system (LDAP, SAML, or CAS).
Project3: Bitbucket cloud
One downside, however, is that Bitubucket does not include support for SVN but this can be easily amended migrating the SVN repos to Git with tools such as SVN Mirror for Bitbucket .
Note: SVN is a centralized version control system.
Incorrect Answers:
Bitbucket:
Bitbucket comes as a distributed version control system based on Git.
Note: A source control system, also called a version control system, allows developers to collaborate on code and track changes. Source control is an essential tool for multi-developer projects.
Our systems support two types of source control: Git (distributed) and Team Foundation Version Control (TFVC). TFVC is a centralized, client-server system. In both Git and TFVC, you can check in files and organize files in folders, branches, and repositories.
References:
https://www.azuredevopslabs.com/labs/azuredevops/yaml/
https://enterprise.github.com/faq

Question: 96

Your team uses an agile development approach.
You need to recommend a branching strategy for the team's Git repository. The strategy must meet the following requirements.
Provide the ability to work on multiple independent tasks in parallel.
Ensure that checked-in code remains in a releasable state always.
Ensure that new features can be abandoned at any time.
Encourage experimentation.
What should you recommend?

A. a single long-running branch
B. multiple long-running branches
C. a single fork per team member
D. a single-running branch with multiple short-lived topic branches

Answer: D

Explanation:
Topic branches, however, are useful in projects of any size. A topic branch is a short-lived branch that you create and use for a single particular feature or related work. This is something you've likely never done with a VCS before because it's generally too expensive to create and merge branches. But in Git it's common to create, work on, merge, and delete branches several times a day.
Reference:
https://git-scm.com/book/en/v2/Git-Branching-Branching-Workflows

Question: 97

Your company has a project in Azure DevOps for a new web application.
The company identifies security as one of the highest priorities.
You need to recommend a solution to minimize the likelihood that infrastructure credentials will be leaked.
What should you recommend?

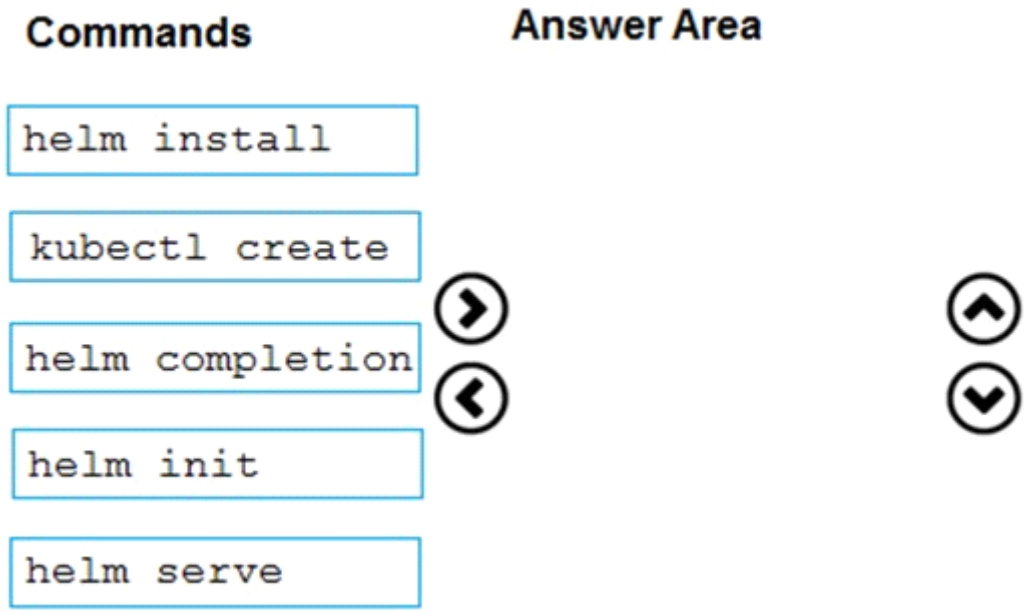
A. Add a Run Inline Azure PowerShell task to the pipeline.
B. Add a PowerShell task to the pipeline and run Set-AzureKeyVaultSecret.
C. Add a Azurre Key Vault task to the pipeline.
D. Add Azure Key Vault references to Azure Resource Manger templates.

Answer: B

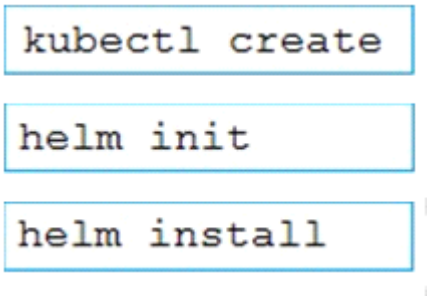
Explanation:
Azure Key Vault provides a way to securely store credentials and other keys and secrets.
The Set-AzureKeyVaultSecret cmdlet creates or updates a secret in a key vault in Azure Key Vault.
References:
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecret

Question: 98

You provision an Azure Kubernetes Service (AKS) cluster that has RBAC enabled. You have a Helm chart for a client application.
You need to configure Helm and Tiller on the cluster and install the chart.
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.



Answer:



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

Question: 99

You have a project in Azure DevOps. You have an Azure Resource Group deployment project in Microsoft
Visual Studio that is checked in to the Azure DevOps project.
You need to create a release pipeline that will deploy resources by using Azure Resource Manager templates.
The solution must minimize administrative effort.
Which task type should you include in the solution?

A. Azure Cloud Service Deployment
B. Azure RM Web App Deployment
C. Azure PowerShell
D. Azure App Service Manage

Answer: C

Explanation:

There are two different ways to deploy templates to Azure DevOps Services. Both methods provide the same
results, so choose the one that best fits your workflow.
1. Add a single step to your build pipeline that runs the PowerShell script that's included in the Azure Resource Group deployment project (Deploy-AzureResourceGroup.ps1). The script copies artifacts and then deploys the template.
2. Add multiple Azure DevOps Services build steps, each one performing a stage task.
The first option has the advantage of using the same script used by developers in Visual Studio and providing
consistency throughout the lifecycle.
References:
https://docs.microsoft.com/en-us/azure/vs-azure-tools-resource-groups-ci-in-vsts

Question: 100

You have an Azure DevOps organization named Contoso and an Azure DevOps project named Project1.
You plan to use Microsoft-hosted agents to build container images that will host full Microsoft .NET Framework apps in a YAML pipeline in Project1.
What are two possible virtual machine images that you can use for the Microsoft-hosted agent pool? Each
correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. vs2017-win2016
B. ubuntu-16.04
C. win1803
D. macOS-10.13
E. vs.2015-win2012r2

Answer: AE

https://github.com/microsoft/azure-pipelines-image-generation/blob/d80f81d6c98f8ce2c74b034309bb774ea8d31cfb/images/win/Vs2015-Server2012R2-Readme.md
https://github.com/actions/virtual-environments/blob/master/images/win/Windows2016-Readme.md

Question: 101

You currently use JIRA, Jenkins, and Octopus as part of your DevOps processes.
You plan to use Azure DevOps to replace these tools.
Which Azure DevOps service should you use to replace each tool? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

JIRA:

- Boards
- Build pipelines
- Release pipelines
- Repos

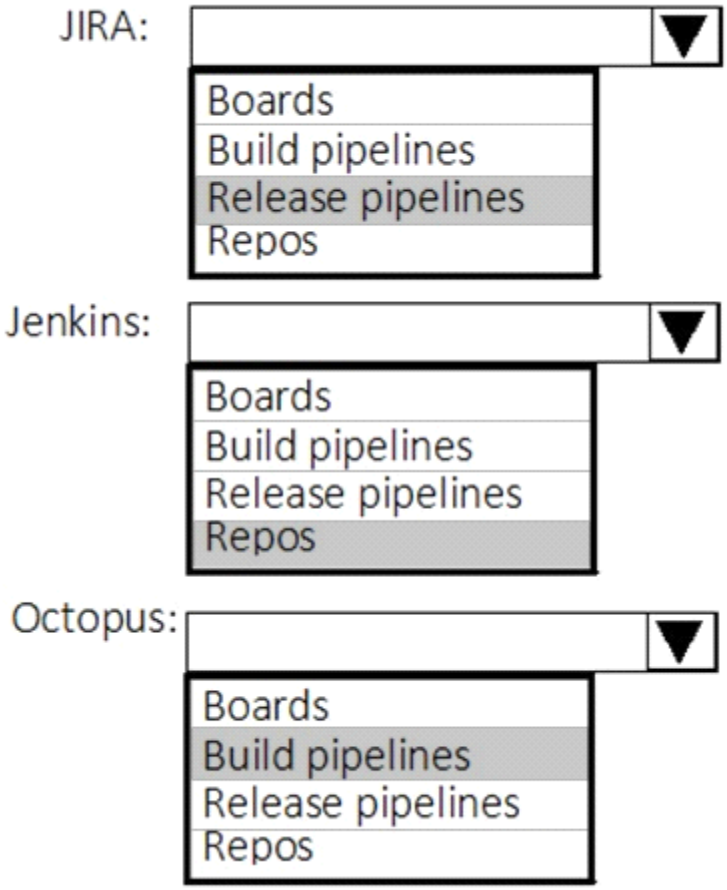
Jenkins:

- Boards
- Build pipelines
- Release pipelines
- Repos

Octopus:

- Boards
- Build pipelines
- Release pipelines
- Repos

Answer:



Explanation:
JIRA: Release pipelines
Atlassian's Jira Software is a popular application that helps teams to plan, track, and manage software releases, whereas Octopus Deploy helps teams automate their development and operations processes in a fast, repeatable, and reliable manner. Together, they enable teams to get better end-to-end visibility into their software pipelines from idea to production.
Jenkins: Repos
One way to integrate Jenkins with Azure Pipelines is to run CI jobs in Jenkins separately. This involves configuration of a CI pipeline in Jenkins and a web hook in Azure DevOps that invokes the CI process when source code is pushed to a repository or a branch.
Octopus: Build pipelines
References:
https://octopus.com/blog/octopus-jira-integration
https://www.azuredevopslabs.com/labs/vstsextend/jenkins/

Question: 102

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:
Two resource groups
Four Azure virtual machines in one resource group
Two Azure SQL databases in other resource group
You need to recommend a solution to deploy the resources.
Solution: Create a single standalone template that will deploy all the resources.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Use two templates, one for each resource group, and link the templates.
References:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-linked-templates

Question: 103

Your company has an Azure subscription.
The company requires that all resource group in the subscription have a tag named organization set to a value of Contoso.
You need to implement a policy to meet the tagging requirement.
How should you complete the policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
{
 "policyRule": {
   "if": {
     "allOf": [
       {
        "field": "type",
        "equals":
       ,
       {
        "not": {
          "field": "tags['organization']",
          "equals": "Contoso"
        }
       }
      ]
    },

    "then": {
      "effect":

      "details": [
        {
          "field": "tags['organizatíon']",
          "value": "Contoso"
        }
       ]
      }
     }
    }
```

"MicrosoftResources/deployments"
"MicrosoftResources/subscriptions"
"MicrosoftResources/subscriptions/resourceGroups"

"Append",
"Deny",
"DeployIfNotExists",

Answer:

Explanation:
Box 1: " Microsoft.Resources/subscriptions/resourceGroups"
Box 2: "Deny",
Sample - Enforce tag and its value on resource groups
},
"policyRule": {
"if": {
"allOf": [
{
"field": "type",
"equals": "Microsoft.Resources/subscriptions/resourceGroups"
},
{
"not": {
"field": "[concat('tags[',parameters('tagName'), ']')]",
"equals": "[parameters('tagValue')]"
}

```
    }
  ]
  },
  "then": {
  "effect": "deny"
  }
  }
  }
}
```

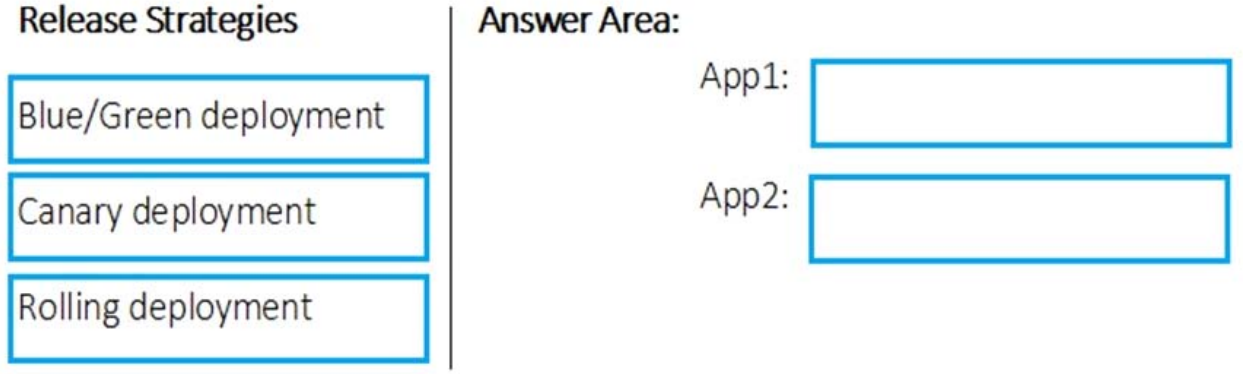
References:
https://docs.microsoft.com/en-us/azure/governance/policy/samples/enforce-tag-on-resource-groups

Question: 104

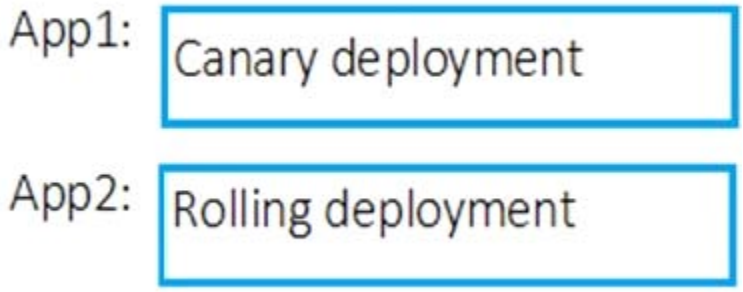
You are defining release strategies for two applications as shown in the following table.

Application name	Goal
App1	Failure of App1 has a major impact on your company. You need a small group of users, who opted in to a testing App1, to test new releases of the application.
App2	You need to minimize the time it takes to deploy new releases of App2, and you must be able to roll back as quickly as possible.

Which release strategy should you use for each application? To answer, drag the appropriate release strategies to the correct applications. Each release strategy 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.



Answer:



Explanation:
App1: Canary deployment
With canary deployment, you deploy a new application code in a small part of the production infrastructure. Once the application is signed off for release, only a few users are routed to it. This minimizes any impact.
With no errors reported, the new version can gradually roll out to the rest of the infrastructure.
App2: Rolling deployment:
In a rolling deployment, an application's new version gradually replaces the old one. The actual deployment happens over a period of time. During that time, new and old versions will coexist without affecting functionality or user experience. This process makes it easier to roll back any new component incompatible with the old components.
Incorrect Answers:
Blue/Green deployment
A blue/green deployment is a change management strategy for releasing software code. Blue/green deployments, which may also be referred to as A/B deployments require two identical hardware environments that are configured exactly the same way. While one environment is active and serving end users, the other environment remains idle.
Blue/green deployments are often used for consumer-facing applications and applications with critical uptime requirements. New code is released to the inactive environment, where it is thoroughly tested. Once the code has been vetted, the team makes the idle environment active, typically by adjusting a router configuration to redirect application program traffic. The process reverses when the next software iteration is ready for release.
References:
https://dev.to/mostlyjason/intro-to-deployment-strategies-blue-green-canary-and-more-3a3

Question: 105

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 Post-deployment conditions, you modify the Timeout setting for post-deployment approvals.
Does this meet the goal?

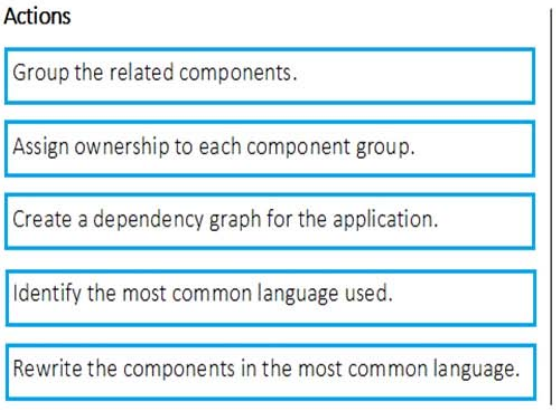
A. Yes
B. No

Answer: B

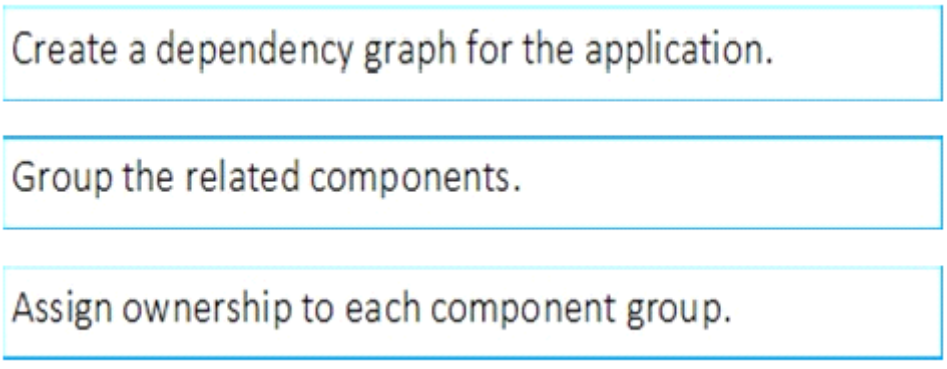
Explanation:
Use Pre-deployments conditions instead.
Use a gate instead of an approval instead.
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates

Question: 106

You need to find and isolate shared code. The shared code will be maintained in a series of packages.
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.



Answer:



Explanation:

Step 1: Create a dependency graph for the application
By linking work items and other objects, you can track related work, dependencies, and changes made over time. All links are defined with a specific link type. For example, you can use Parent/Child links to link work items to support a hierarchical tree structure. Whereas, the Commit and Branch link types support links between work items and commits and branches, respectively.
Step 2: Group the related components.
Packages enable you to share code across your organization: you can compose a large product, develop multiple products based on a common shared framework, or create and share reusable components and libraries.
Step 3: Assign ownership to each component graph
References:
https://docs.microsoft.com/en-us/azure/devops/boards/queries/link-work-items-support-traceability?view=azure-devops&tabs=new-web-form
https://docs.microsoft.com/en-us/visualstudio/releasenotes/tfs2017-relnotes

Question: 107

You have an application that consists of several Azure App Service web apps and Azure functions.
You need to access the security of the web apps and the functions.
Which Azure features can you use to provide a recommendation for the security of the application?

A. Security & Compliance in Azure Log Analytics
B. Resource health in Azure Service Health
C. Smart Detection in Azure Application Insights
D. Compute & apps in Azure Security Center

Answer: D

Explanation:
Monitor compute and app services: Compute & apps include the App Services tab, which App services: list of your App service environments and current security state of each.
Recommendations
This section has a set of recommendations for each VM and computer, web and worker roles, Azure App Service Web Apps, and Azure App Service Environment that Security Center monitors. The first column lists the recommendation. The second column shows the total number of resources that are affected by that recommendation. The third column shows the severity of the issue.
Incorrect Answers:
C: Smart Detection automatically warns you of potential performance problems, not security problems in your web application.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-diagnostics

Question: 108

You have a private distribution group that contains provisioned and unprovisioned devices.
You need to distribute a new iOS application to the distribution group by using Microsoft Visual Studio App Center.

What should you do?

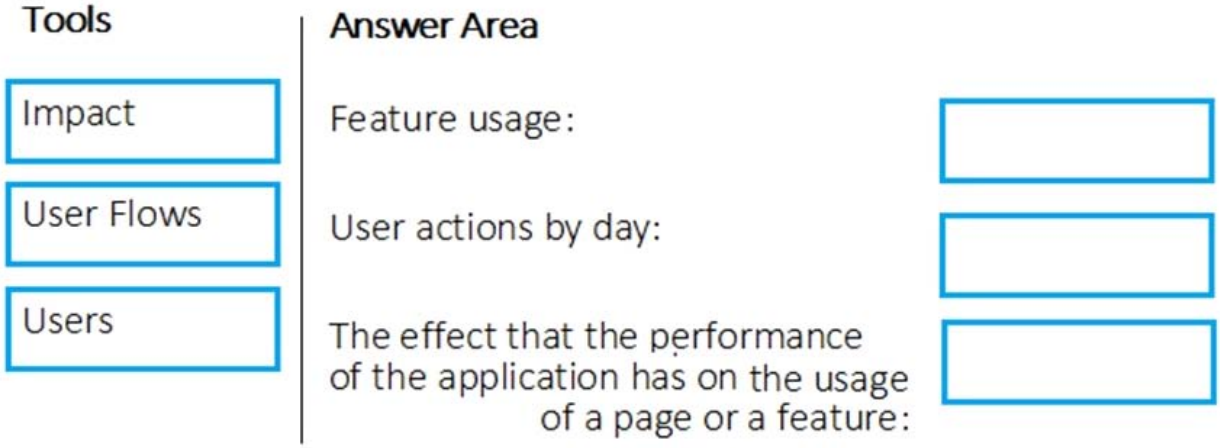
A. Request the Apple ID associated with the user of each device.
B. Register the devices on the Apple Developer portal.
C. Create an active subscription in App Center Test.
D. Add the device owner to the organization in App Center.

Answer: B

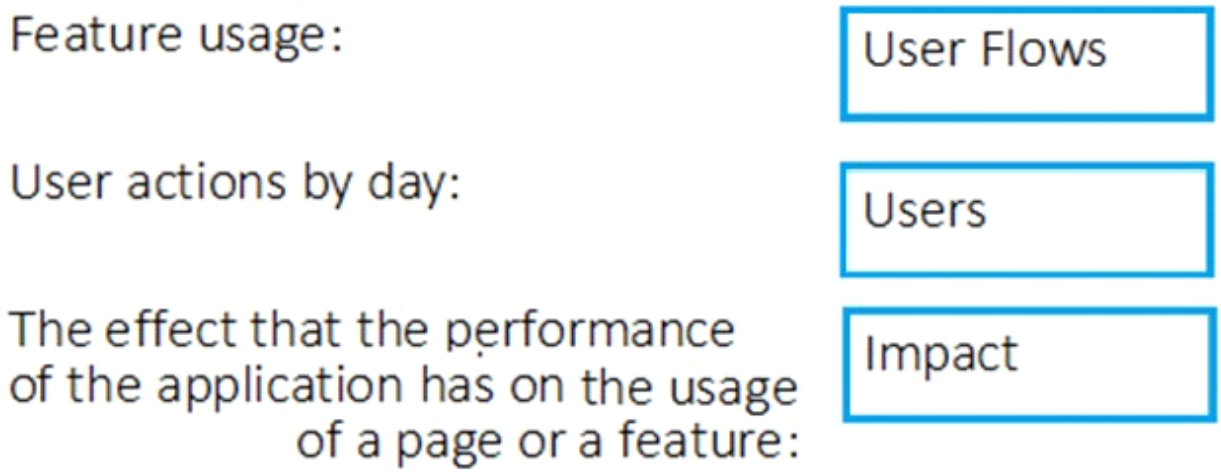
Explanation:
When releasing an iOS app signed with an ad-hoc or development provisioning profile, you must obtain tester's device IDs (UDIDs), and add them to the provisioning profile before compiling a release. When you enable the distribution group's Automatically manage devices setting, App Center automates the before mentioned operations and removes the constraint for you to perform any manual tasks. As part of automating the workflow, you must provide the user name and password for your Apple ID and your production certificate in a .p12 format.
App Center starts the automated tasks when you distribute a new release or one of your testers registers a new device. First, all devices from the target distribution group will be registered, using your Apple ID, in your developer portal and all provisioning profiles used in the app will be generated with both new and existing device ID. Afterward, the newly generated provisioning profiles are downloaded to App Center servers.
References:
https://docs.microsoft.com/en-us/appcenter/distribution/groups

Question: 109

Your company wants to use Azure Application Insights to understand how user behaviors affect an application.
Which application Insights tool should you use to analyze each behavior? To answer, drag the appropriate tools to the correct behaviors. Each 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.



Answer:



Explanation:
Box 1: User Flows
The User Flows tool visualizes how users navigate between the pages and features of your site. It's great for answering questions like:
How do users navigate away from a page on your site?
What do users click on a page on your site?
Where are the places that users churn most from your site?
Are there places where users repeat the same action over and over?
Box 2: Users
Box 3: Impact
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-flows

Question: 110

You have a GitHub repository.
You create a new repository in Azure DevOps.
You need to recommend a procedure to clone the repository from GitHub to Azure DevOps.
What should you recommend?

A. Create a pull request.
B. Create a webhook.
C. Create a service connection for GitHub.
D. From Import a Git repository, click Import.
E. Create a personal access token in Azure DevOps.

Answer: D

Explanation:
You can import an existing Git repo from GitHub, Bitbucket, GitLab, or other location into a new or empty existing repo in your project in Azure DevOps.
Import into a new repo
Select Repos, Files.

From the repo drop-down, select Import repository.
If the source repo is publicly available, just enter the clone URL of the source repository and a name for your new Git repository.
References:
https://docs.microsoft.com/en-us/azure/devops/repos/git/import-git-repository?view=azure-devops

Question: 111

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 need to recommend an integration strategy for the build process of a Java application. The solution must
meet the following requirements:
The builds must access an on-premises dependency management system.
The build outputs must be stored as Server artifacts in Azure DevOps.
The source code must be stored in a Git repository in Azure DevOps.
Solution: Configure an Octopus Tentacle on an on-premises machine. Use the Package Application task in the build pipeline.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Octopus Deploy is an automated deployment server that makes it easy to automate deployment of ASP.NET web applications, Java applications, NodeJS application and custom scripts to multiple environments.
Octopus can be installed on various platforms including Windows, Mac and Linux. It can also be integrated with most version control tools including VSTS and GIT.
When you deploy software to Windows servers, you need to install Tentacle, a lightweight agent service, on your Windows servers so they can communicate with the Octopus server.
When defining your deployment process, the most common step type will be a package step. This step deploys your packaged application onto one or more deployment targets.
When deploying a package you will need to select the machine role that the package will be deployed to.
References:
https://octopus.com/docs/deployment-examples/package-deployments
https://explore.emtecinc.com/blog/octopus-for-automated-deployment-in-devops-models

Question: 112

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 need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:
The builds must access an on-premises dependency management system.
The build outputs must be stored as Server artifacts in Azure DevOps.
The source code must be stored in a Git repository in Azure DevOps.
Solution: Install and configure a self-hosted build agent on an on-premises machine. Configure the build pipeline to use the Default agent pool. Include the Java Tool Installer task in the build pipeline.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use Octopus Tentacle.
References:
https://explore.emtecinc.com/blog/octopus-for-automated-deployment-in-devops-models

Question: 113

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 need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:
The builds must access an on-premises dependency management system.
The build outputs must be stored as Server artifacts in Azure DevOps.
The source code must be stored in a Git repository in Azure DevOps.
Solution: Configure the build pipeline to use a Hosted VS 2017 agent pool. Include the Java Tool Installer task in the build pipeline.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Instead use Octopus Tentacle.
References:
https://explore.emtecinc.com/blog/octopus-for-automated-deployment-in-devops-models

Question: 114

You are designing the development process for your company.
You need to recommend a solution for continuous inspection of the company's code base to locate common code patterns that are known to be problematic.
What should you include in the recommendation?

A. Microsoft Visual Studio test plans
B. Gradle wrapper scripts
C. SonarCloud analysis
D. the JavaScript task runner

Answer: C

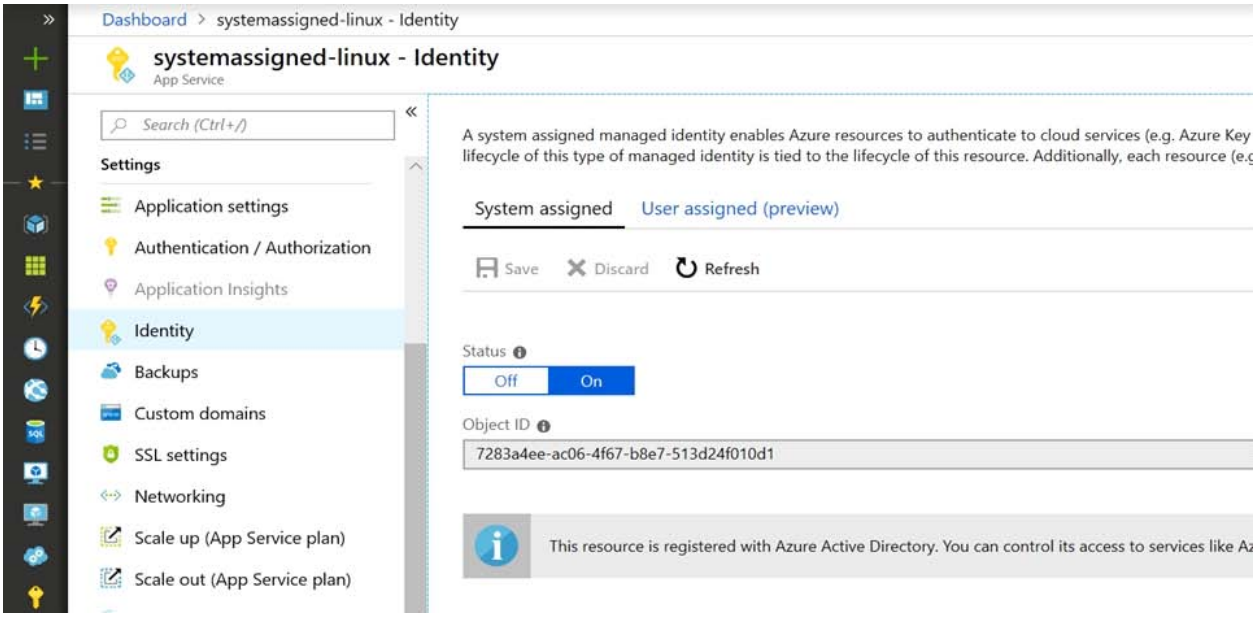
Explanation:
SonarCloud is a cloud service offered by SonarSource and based on SonarQube. SonarQube is a widely adopted open source platform to inspect continuously the quality of source code and detect bugs, vulnerabilities and code smells in more than 20 different languages.
Note: The SonarCloud Azure DevOps extension brings everything you need to have your projects analyzed on SonarCloud very quickly.
Incorrect Answers:
A: Test plans are used to group together test suites and individual test cases. This includes static test suites, requirement-based suites, and query-based suites.
References:
https://docs.travis-ci.com/user/sonarcloud/
https://sonarcloud.io/documentation/integrations/vsts/

Question: 115

You need to ensure that an Azure web app named az400-9940427-main can retrieve secrets from an Azure key vault named az400-9940427-kv1 by using a system managed identity.
The solution must use the principle of least privilege.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
1. In Azure portal navigate to the az400-9940427-main app.
2. Scroll down to the Settings group in the left navigation.
3. Select Managed identity.
4. Within the System assigned tab, switch Status to On. Click Save.



References:
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity

Question: 116

Your company is building a new solution in Java.
The company currently uses a SonarQube server to analyze the code of .NET solutions.
You need to analyze and monitor the code quality of the Java solution.
Which task types should you add to the build pipeline?

A. Chef
B. Gradle
C. Octopus
D. Gulp

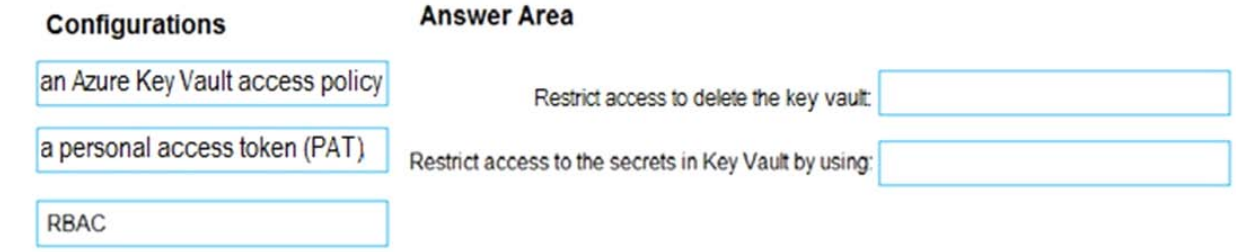
Answer: B

Explanation:
SonarQube is a set of static analyzers that can be used to identify areas of improvement in your code. It allows you to analyze the technical debt in your project and keep track of it in the future. With Maven and Gradle build tasks, you can run SonarQube analysis with minimal setup in a new or existing Azure DevOps Services build task.
References:
https://docs.microsoft.com/en-us/azure/devops/java/sonarqube?view=azure-devops

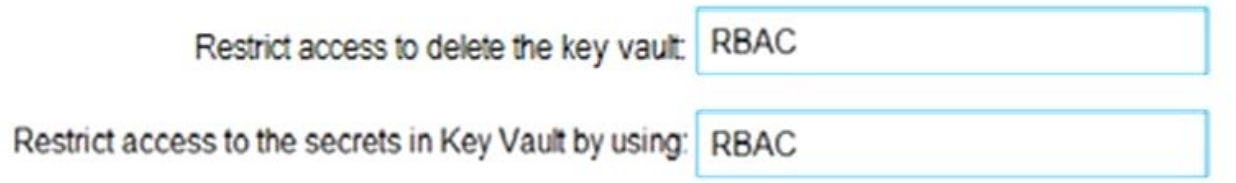
Question: 117

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.



Answer:



Explanation:
Box 1: RBAC
Management plane access control uses RBAC.
The management plane consists of operations that affect the key vault itself, such as:
Creating or deleting a key vault.
Getting a list of vaults in a subscription.
Retrieving Key Vault properties (such as SKU and tags).
Setting Key Vault access policies that control user and application access to keys and secrets.
Box 2: RBAC
References:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-tutorial-use-key-vault

Question: 118

You have an Azure function hosted in an App Service plan named az400-9940427-func1.
You need to configure az400-9940427-func1 to upgrade the functions automatically whenever new code is committed to the master branch of https://github.com/Azure-Samples/functions-quickstart.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
1. Open Microsoft Azure Portal
2. Log into your Azure account, select App Services in the Azure portal left navigation, and then select configure az400-9940427-func1.

3. On the app page, select Deployment Center in the left menu.
4. On the Build provider page, select Azure Pipelines (Preview), and then select Continue.
5. On the Configure page, in the Code section:
For GitHub, drop down and select the Organization, Repository, and Branch you want to deploy continuously.
6. Select Continue.
7. On the Test page, choose whether to enable load tests, and then select Continue.
8. Depending on your App Service plan pricing tier, you may see a Deploy to staging page. Choose whether to enable deployment slots, and then select Continue.
9. After you configure the build provider, review the settings on the Summary page, and then select Finish.
References:
https://docs.microsoft.com/en-us/azure/app-service/deploy-continuous-deployment

Question: 119

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 Azure DevOps project.
Your build process creates several artifacts.
You need to deploy the artifacts to on-premises servers.
Solution: You deploy a Kubernetes cluster on-premises. You deploy a Helm agent to the cluster. You add a Download Build Artifacts task to the deployment pipeline.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead you should deploy an Azure self-hosted agent to an on-premises server.
Note: To build your code or deploy your software using Azure Pipelines, you need at least one agent.
If your on-premises environments do not have connectivity to a Microsoft-hosted agent pool (which is typically the case due to intermediate firewalls), you'll need to manually configure a self-hosted agent on on-premises computer(s).
Note 2: As we [Microsoft] are launching this new experience in preview, we are currently optimizing it for Azure Kubernetes Service (AKS) and Azure Container Registry (ACR). Other Kubernetes clusters, for example running on-premises or in other clouds, as well as other container registries, can be used, but require setting up a Service Account and connection manually.
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops

Question: 120

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 Azure DevOps project.
Your build process creates several artifacts.
You need to deploy the artifacts to on-premises servers.
Solution: You deploy a Docker build to an on-premises server. You add a Download Build Artifacts task to the deployment pipeline.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead you should deploy an Azure self-hosted agent to an on-premises server.
Note: To build your code or deploy your software using Azure Pipelines, you need at least one agent.
If your on-premises environments do not have connectivity to a Microsoft-hosted agent pool (which is typically the case due to intermediate firewalls), you'll need to manually configure a self-hosted agent on on-premises computer(s).
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops

Question: 121

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 Azure DevOps project.
Your build process creates several artifacts.
You need to deploy the artifacts to on-premises servers.
Solution: You deploy an Azure self-hosted agent to an on-premises server. You add a Copy and Publish Build Artifacts task to the deployment pipeline.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
To build your code or deploy your software using Azure Pipelines, you need at least one agent.
If your on-premises environments do not have connectivity to a Microsoft-hosted agent pool (which is typically the case due to intermediate firewalls), you'll need to manually configure a self-hosted agent on on-premises computer(s). The agents must have connectivity to the target on-premises environments, and access to the Internet to connect to Azure Pipelines or Team Foundation Server.
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops

Question: 122

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 fall to meet the performance baseline?

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

Answer: C

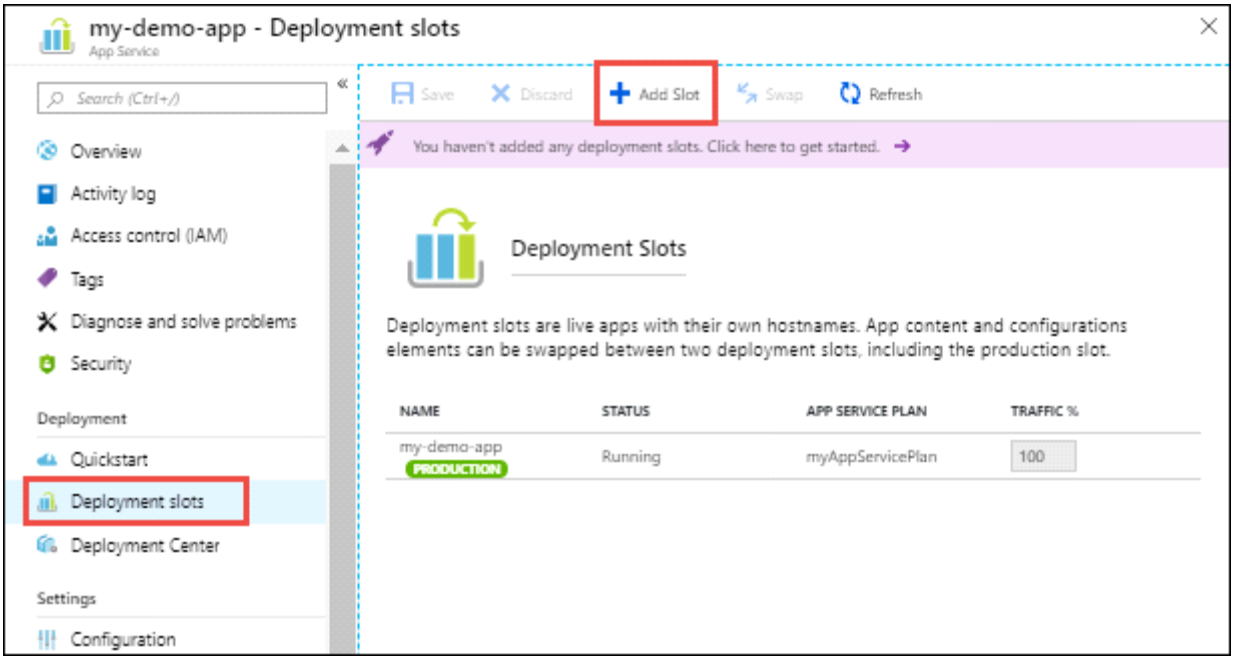
Explanation:
Scenarios and use cases for gates include:
Quality validation. Query metrics from tests on the build artifacts such as pass rate or code coverage and deploy only if they are within required thresholds.
Use Quality Gates to integrate monitoring into your pre-deployment or post-deployment. This ensures that you are meeting the key health/performance metrics (KPIs) as your applications move from dev to production and any differences in the infrastructure environment or scale is not negatively impacting your KPIs.
Note: 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/en-us/azure/azure-monitor/continuous-monitoring
https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates?view=azure-devops

Question: 123

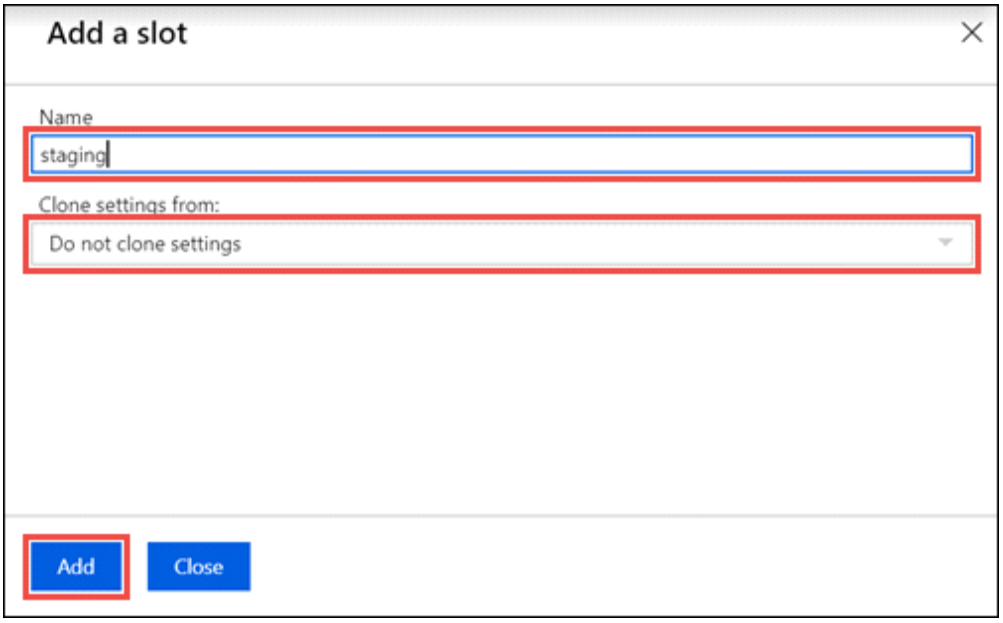
You need to ensure that an Azure web app named az400-9940427-main supports rolling upgrades. The solution must ensure that only 10 percent of users who connect to az400-9940427-main use update versions of the app.
The solution must minimize administrative effort.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
Set up staging environments in Azure App Service
1. Open Microsoft Azure Portal
2. Log into your Azure account, select your app's resource page, in the left pane, select Deployment slots > Add Slot.

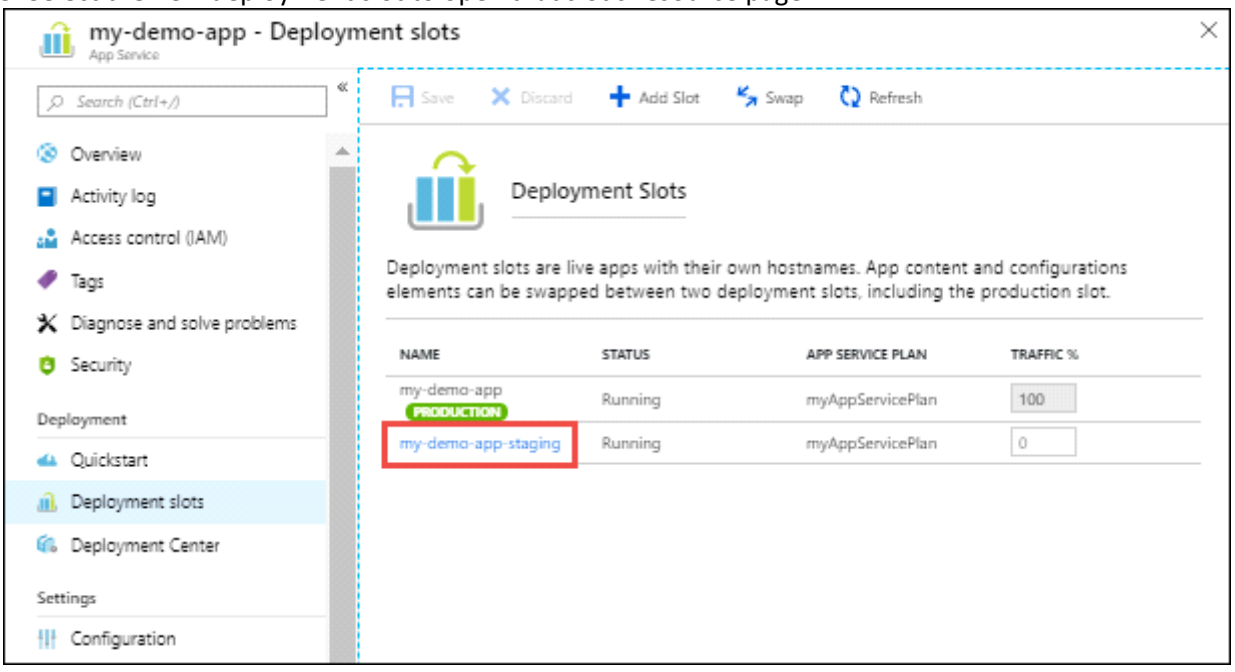


3. In the Add a slot dialog box, give the slot a name, and select whether to clone an app configuration from another deployment slot. Select Add to continue.



4. After the slot is added, select Close to close the dialog box. The new slot is now shown on the Deployment slots page. By default, Traffic % is set to 0 for the new slot, with all customer traffic routed to the production slot.

5. Select the new deployment slot to open that slot's resource page.



6. Change TRAFFIC % to 10

References:

https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots

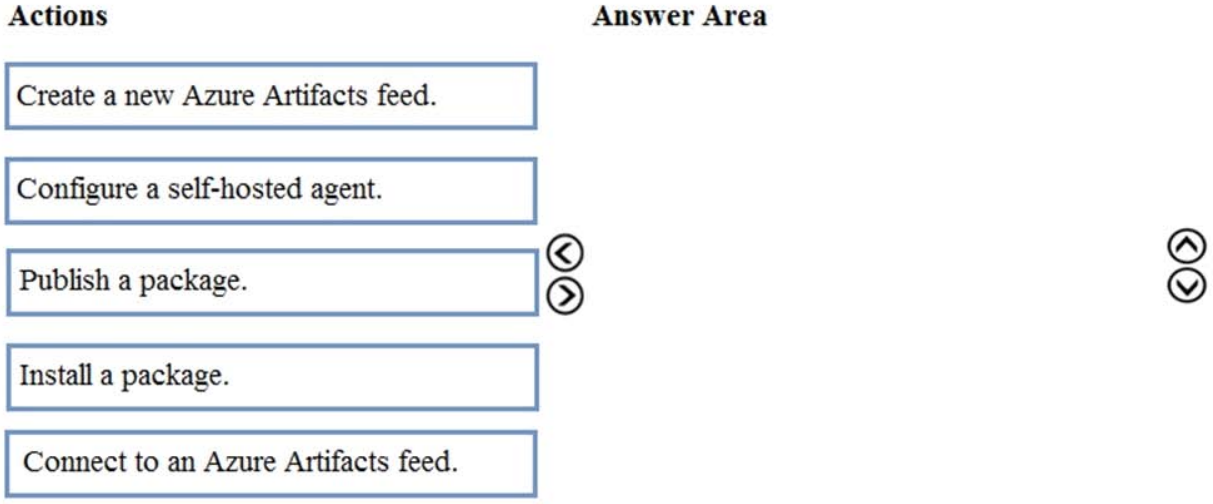
Question: 124

You are creating a NuGet package.

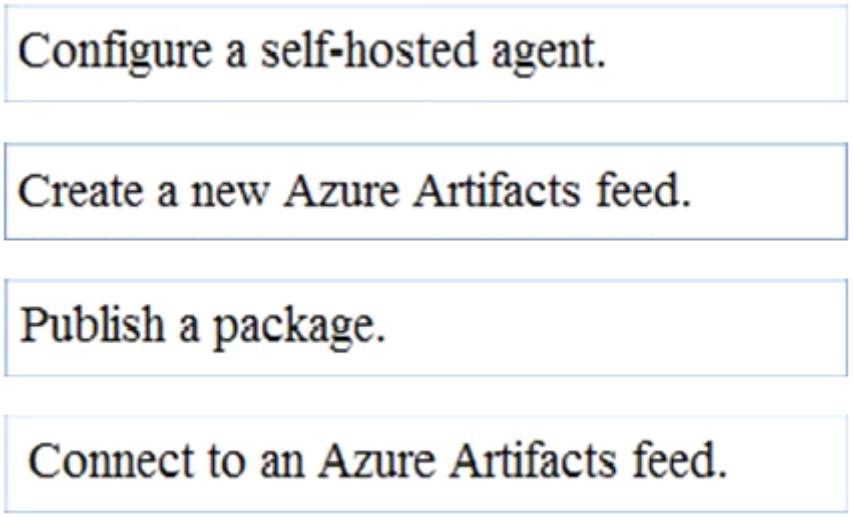
You plan to distribute the package to your development team privately.

You need to share the package and test that the package can be consumed.

Which four 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.



Answer:



Explanation:
Step 1: Configure a self-hosted agent.
The build will run on a Microsoft hosted agent.
Step 2: Create a new Azure Artifacts feed
Microsoft offers an official extension for publishing and managing your private NuGet feeds.
Step 3: Publish the package.
Publish, pack and push the built project to your NuGet feed.
Step 4: Connect to an Azure Artifacts feed.
With the package now available, you can point Visual Studio to the feed, and download the newly published package
References:
https://medium.com/@dan.cokely/creating-nuget-packages-in-azure-devops-with-azure-pipelines-and-yaml-d6fa30f0f15e

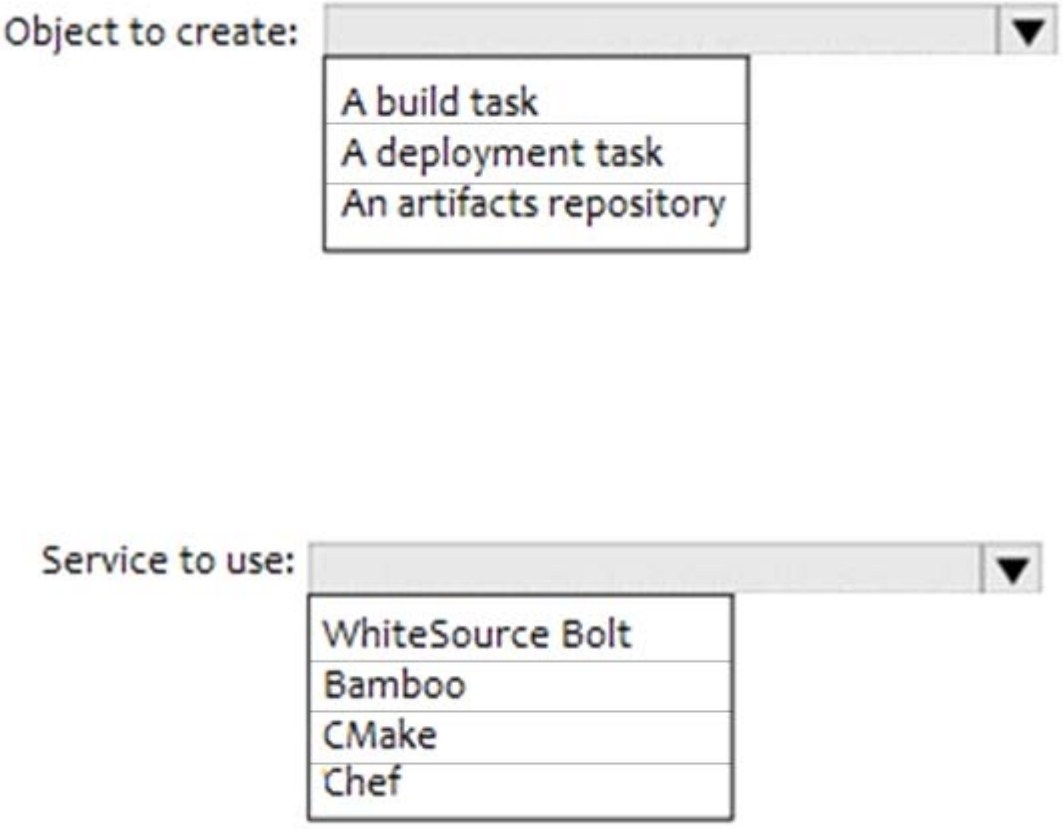
Question: 125

You have an Azure DevOps project that contains a build pipeline. The build pipeline uses approximately 50 open source libraries.

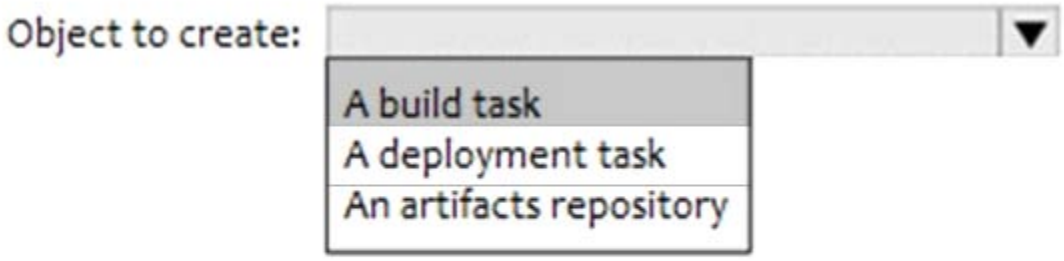
You need to ensure that the project can be scanned for known security vulnerabilities in the open source libraries.

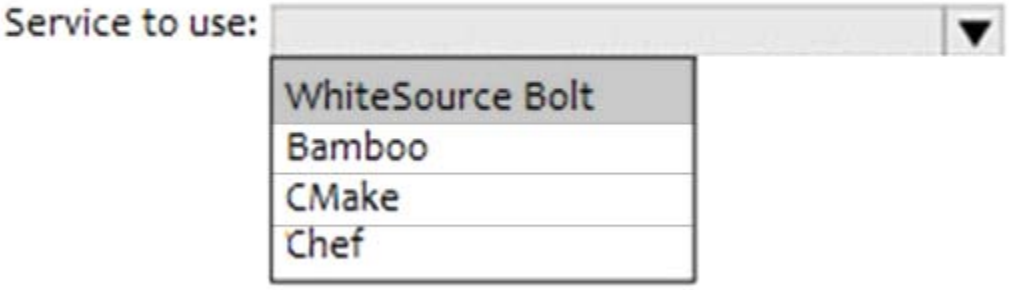
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:





Explanation:
Box 1: A Build task
Trigger a build
You have a Java code provisioned by the Azure DevOps demo generator. You will use WhiteSource Bolt extension to check the vulnerable components present in this code.
Go to Builds section under Pipelines tab, select the build definition WhiteSourceBolt and click on Queue to trigger a build.
To view the build in progress status, click on ellipsis and select View build results.
Box 2: WhiteSource Bolt
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.
References:
https://www.azuredevopslabs.com/labs/vstsextend/whitesource/

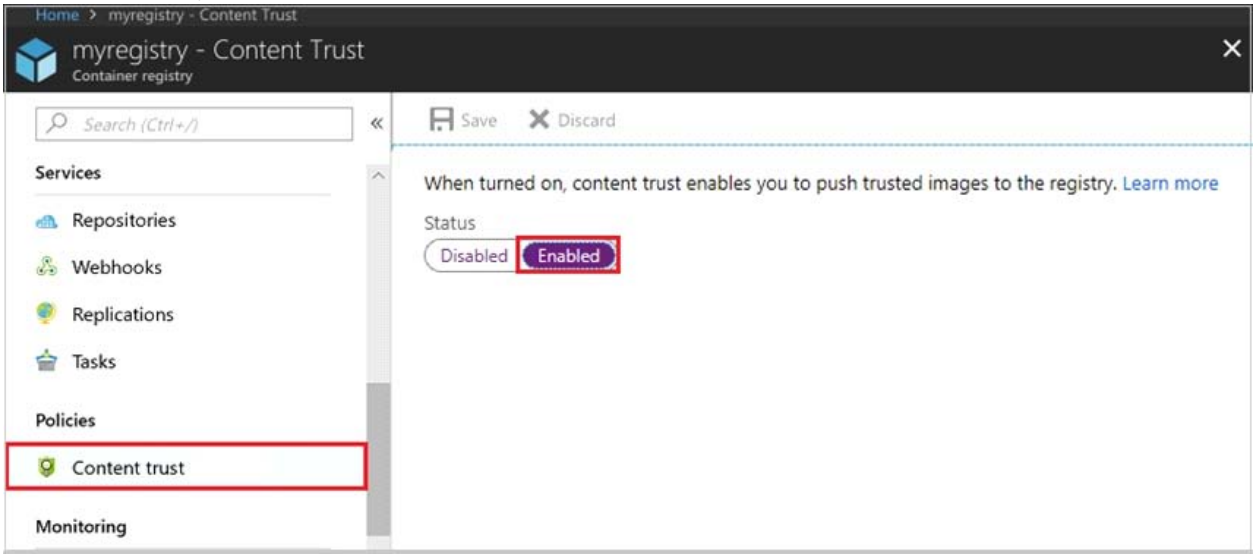
Question: 126

You plane to store signed images in an Azure Container Registry instance named az4009940427acr1.
You need to modify the SKU for az4009940427acr1 to support the planned images. The solution must minimize costs.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:

1. Open Microsoft Azure Portal, and select the Azure Container Registry instance named az4009940427acr1.
2. Under Policies, select Content Trust > Enabled > Save.



References:

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust

Question: 127

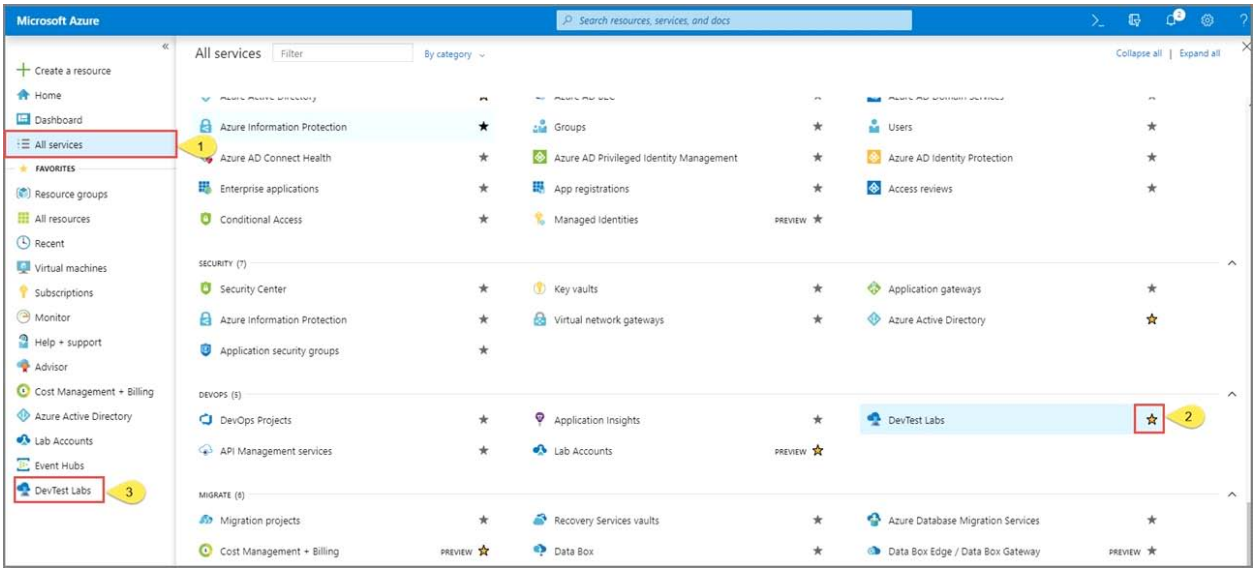
You need to create a virtual machine template in an Azure DevTest Labs environment named az400-9940427-dtl1. The template must be based on Windows Server 2016 Datacenter. Virtual machines created from the template must include the selenium tool and the Google Chrome browser.

To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:

1. Open Microsoft Azure Portal
2. Select All Services, and then select DevTest Labs in the DEVOPS section.



3. From the list of labs, select the az400-9940427-dtl1 lab
4. On the home page for your lab, select + Add on the toolbar.
5. Select the Windows Server 2016 Datacenter base image for the VM.
6. Select automation options at the bottom of the page above the Submit button.
7. You see the Azure Resource Manager template for creating the virtual machine.
8. The JSON segment in the resources section has the definition for the image type you selected earlier.

References:
https://docs.microsoft.com/bs-cyrl-ba/azure//lab-services/devtest-lab-vm-powershell

Question: 128

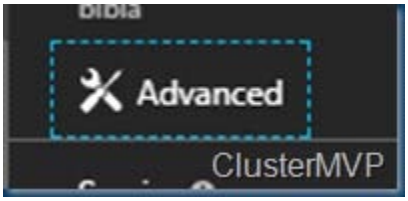
You need to prepare a network security group (NSG) named az400-9940427-nsg1 to host an Azure DevOps pipeline agent. The solution must allow only the required outbound port for Azure DevOps and deny all other inbound and outbound access to the Internet.

To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:

1. Open Microsoft Azure Portal and Log into your Azure account.
2. Select network security group (NSG) named az400-9940427-nsg1
3. Select Settings, Outbound security rules, and click Add
4. Click Advanced



5. Change the following settings:

Destination Port range: 8080

Protocol. TCP

Action: Allow

Note: By default, Azure DevOps Server uses TCP Port 8080.
References:
https://robertsmit.wordpress.com/2017/09/11/step-by-step-azure-network-security-groups-nsg-security-center-azure-nsg-network/
https://docs.microsoft.com/en-us/azure/devops/server/architecture/required-ports?view=azure-devops

Question: 129

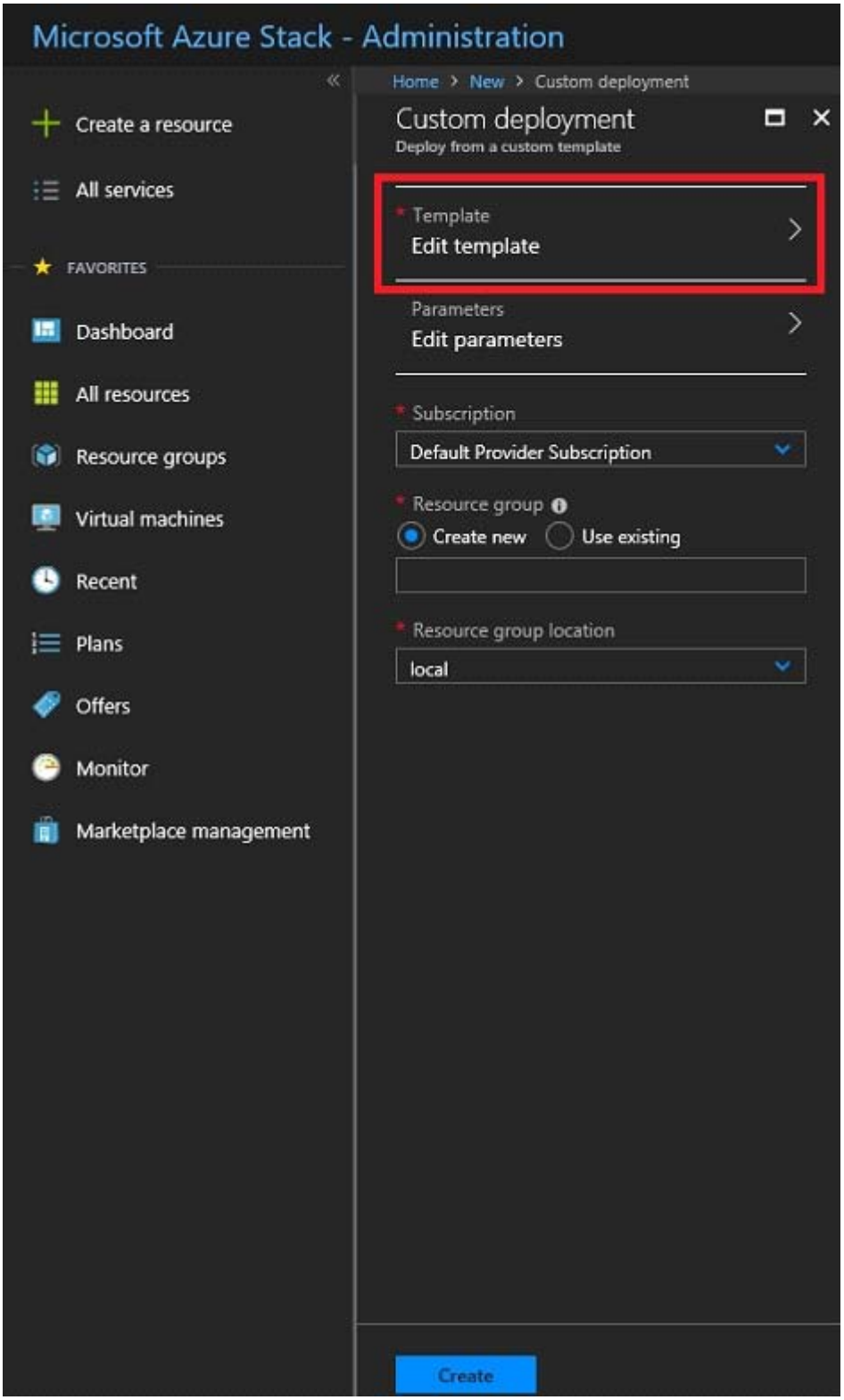
You plan to deploy a template named D:\Deploy.json to a resource group named Deploy-lod9940427.
You need to modify the template to meet the following requirements, and then to deploy the template:
The address space must be reduced to support only 256 total IP addresses.
The subnet address space must be reduced to support only 64 total IP addresses.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

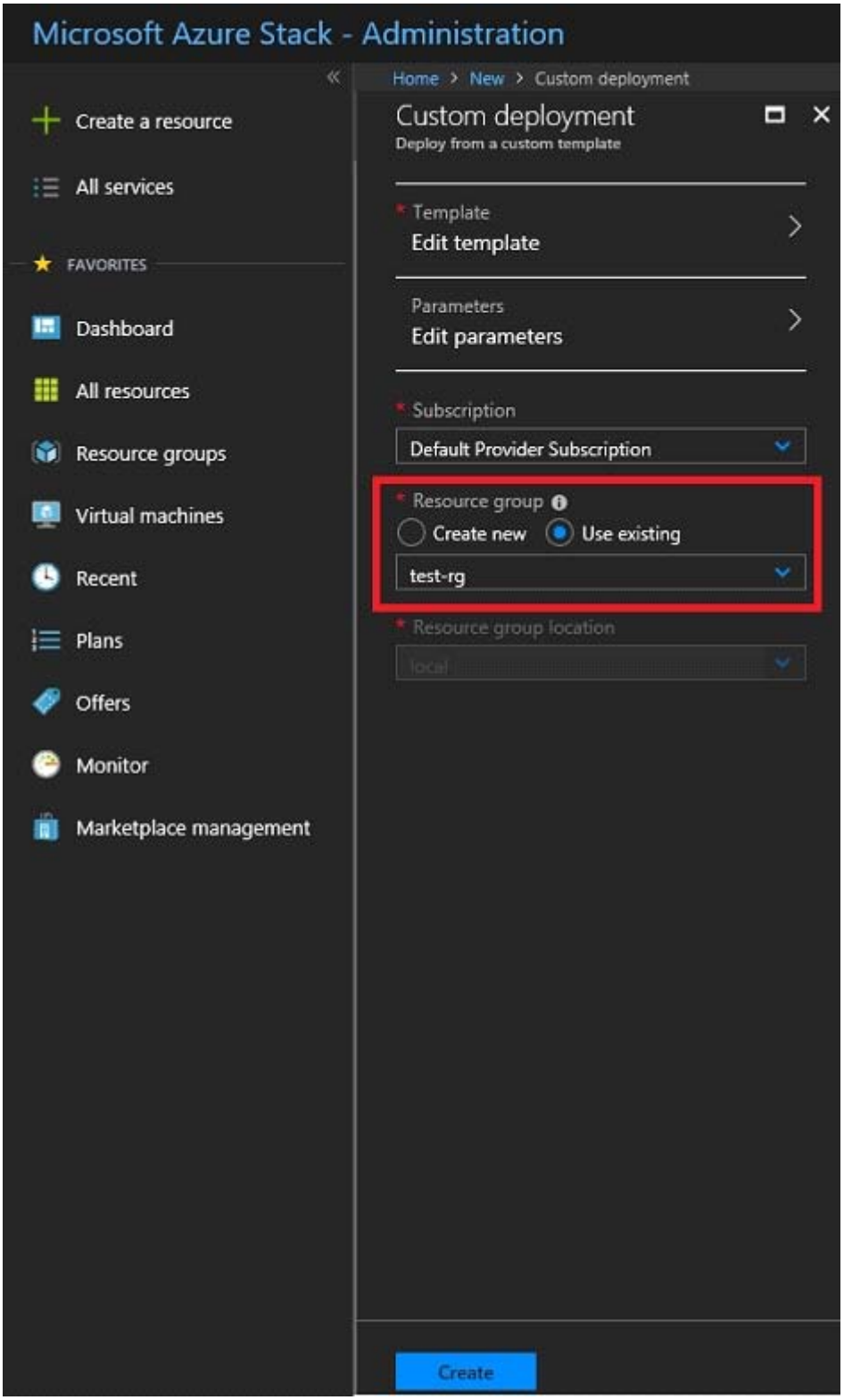
Explanation:
1. Sign in to the portal,
2. Choose template Deploy-lod9940427
3. Select Edit template, and then paste your JSON template code into the code window.
4. Change the ASddressPrefixes to 10.0.0.0/24 in order to support only 256 total IP addresses.
addressSpace":{"addressPrefixes": ["10.0.0.0/24"]},
5. Change the firstSubnet addressprefix to 10.0.0.0/26 to support only 64 total IP addresses.

```
"subnets":[
    {
     "name":"firstSubnet",
     "properties":{
    "addressPrefix":"10.0.0.0/24"
     }
```

6. Select Save.



7. Select Edit parameters, provide values for the parameters that are shown, and then select OK.
8 Select Subscription. Choose the subscription you want to use, and then select OK.
9. Select Resource group. Choose an existing resource group or create a new one, and then select OK.



10. Select Create. A new tile on the dashboard tracks the progress of your template deployment.

References:

https://docs.microsoft.com/en-us/azure-stack/user/azure-stack-deploy-template-portal?view=azs-1908

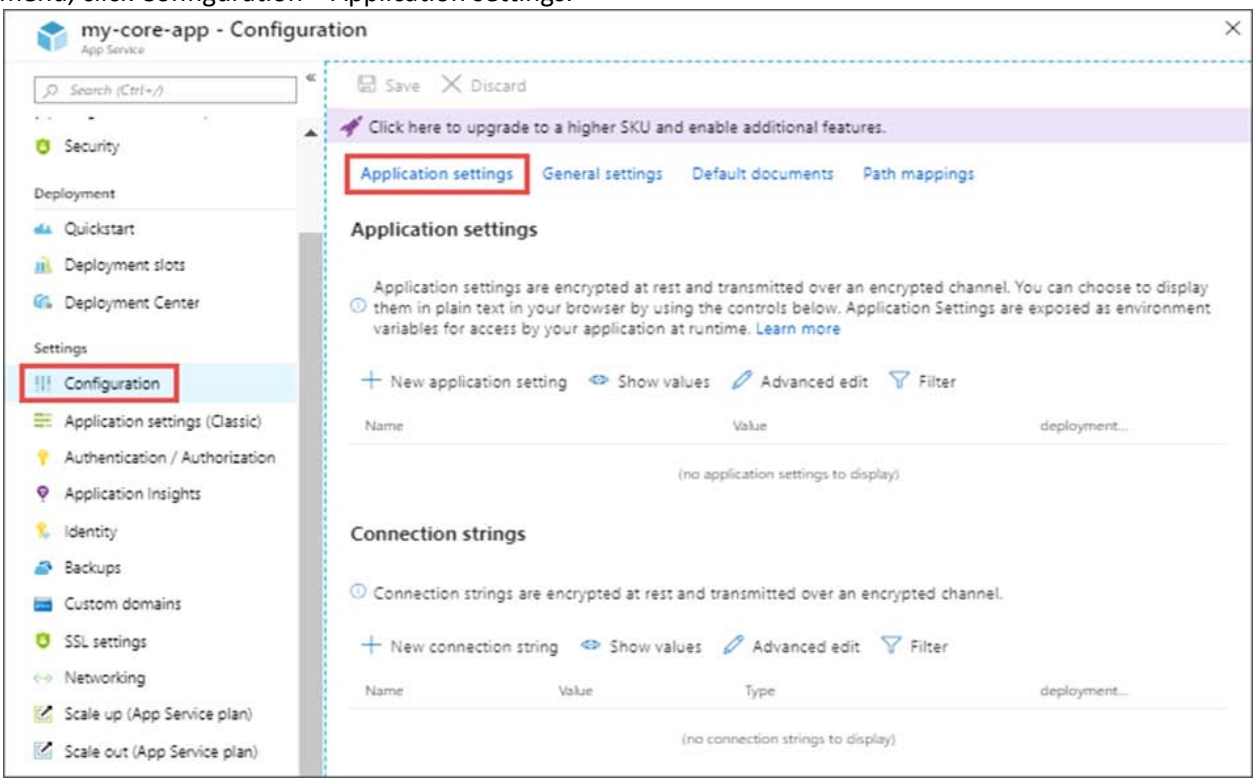
https://docs.microsoft.com/en-us/azure/architecture/building-blocks/extending-templates/update-resource

Question: 130

You need to configure an Azure web app named az400-9940427-main to contain an environmental variable named "MAX_ITEMS". The environmental variable must have a value of 50.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
1. In the Azure portal, navigate to the az400-9940427-main app's management page. In the app's left menu, click Configuration > Application settings.



2. Click New Application settings
3. Enter the following:
Name: MAX_ITEMS
Value: 50
References:
https://docs.microsoft.com/en-us/azure/app-service/configure-common

Question: 131

You have an Azure DevOps project named Project1 and an Azure subscription named Sub1. Sub1 contains an Azure virtual machine scale set named VMSS1. VMSS1 hosts a web application named WebApp1.
WebApp1 uses stateful sessions.

The WebApp1 installation is managed by using the Custom Script extension. The script resides in an Azure Storage account named sa1.
You plan to make a minor change to a UI element of WebApp1 and to gather user feedback about the change.
You need to implement limited user testing for the new version of WebApp1 on VMSS1.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Modify the load balancer settings of VMSS1.
B. Redeploy VMSS1.
C. Upload a custom script file to sa1.
D. Modify the Custom Script extension settings of VMSS1.
E. Update the configuration of a virtual machine in VMSS1.

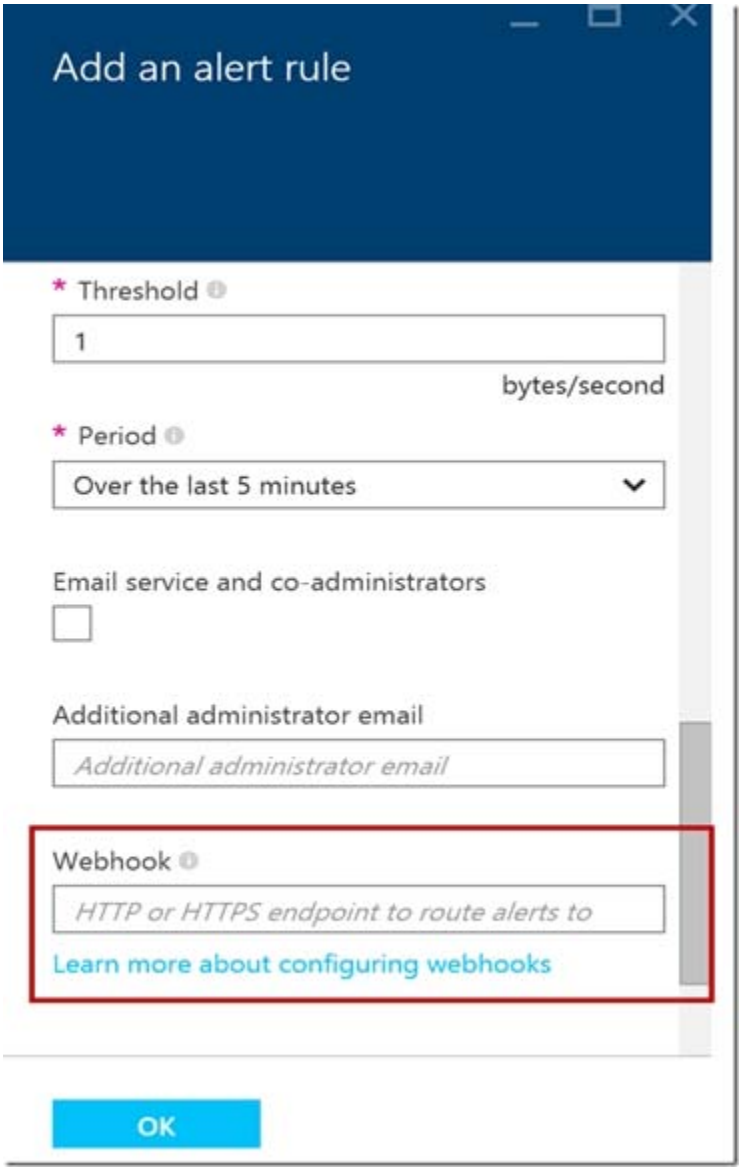
Answer: BCD

Question: 132

You need to create a notification if the peak average response time of an Azure web app named az400-9940427-main is more than five seconds when evaluated during a five-minute period. The notification must trigger the "https://contoso.com/notify" webhook.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
1. Open Microsoft Azure Portal
2. Log into your Azure account and go to App Service and look under Monitoring then you will see Alert.
3. Select Add an alert rule
4. Configure the alert rule as per below and click Ok.
Source: Alert on Metrics
Resource Group: az400-9940427-main
Resource: az400-9940427-main
Threshold: 5
Period: Over the last 5 minutes
Webhook: https://contoso.com/notify



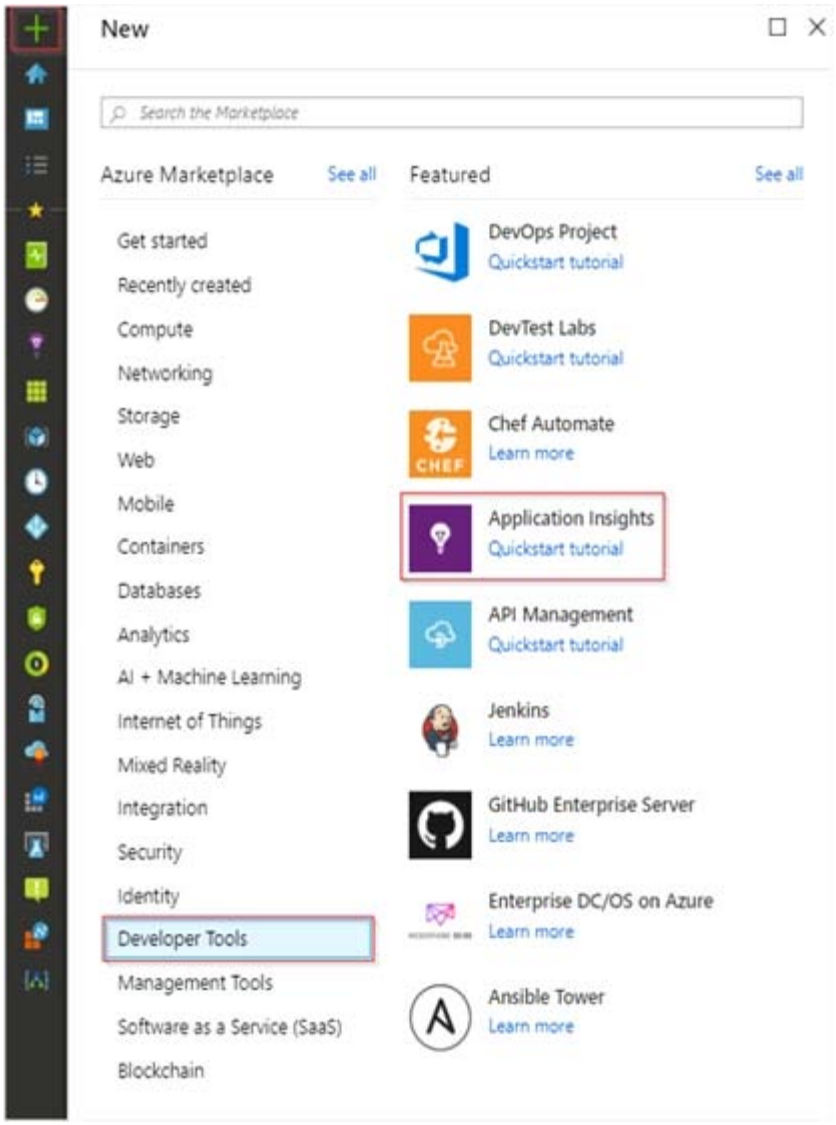
References:
https://azure.microsoft.com/es-es/blog/webhooks-for-azure-alerts/

Question: 133

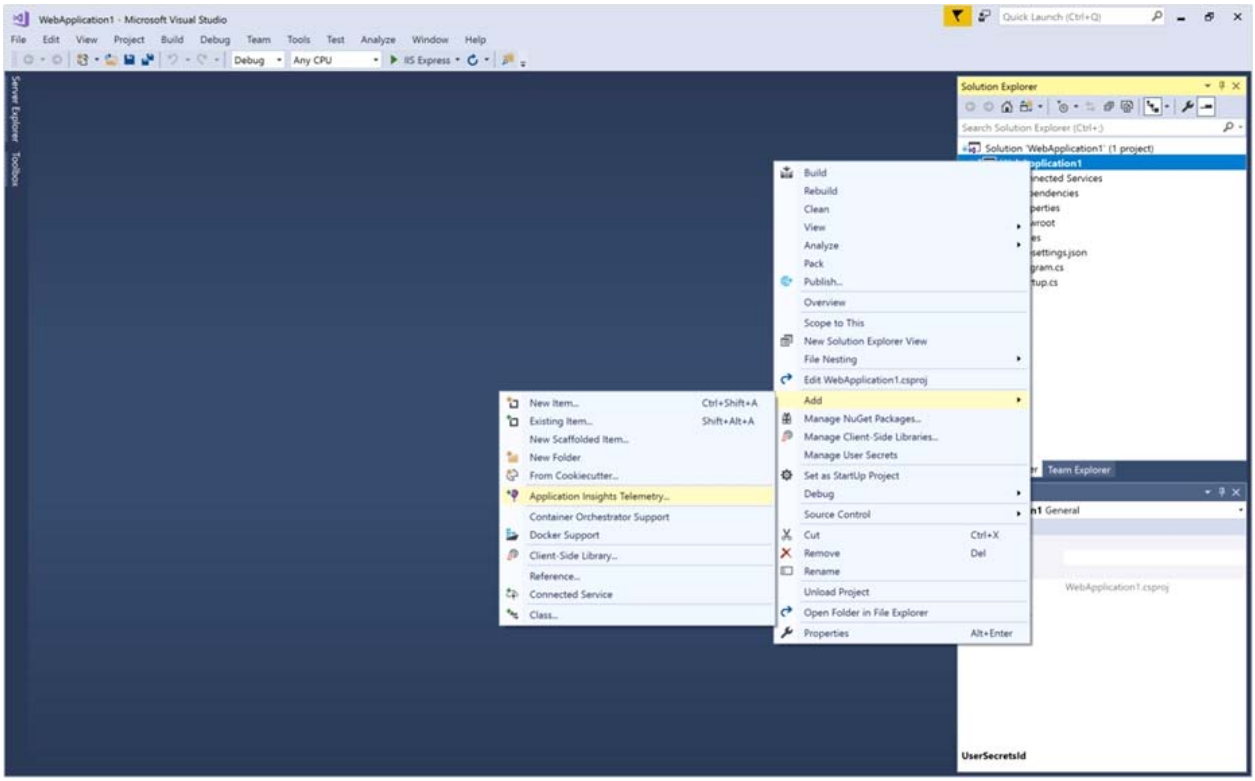
You need to create an instance of Azure Application Insights named az400-9940427-main and configure the instance to receive telemetry data from an Azure web app named az400-9940427-main.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
Step 1: Create an instance of Azure Application Insights
1. Open Microsoft Azure Portal
2. Log into your Azure account, Select Create a resource > Developer tools > Application Insights.



3. Enter the following settings, and then select Review + create.
Name: az400-9940427-main
Step 2: Configure App Insights SDK
4. Open your ASP.NET Core Web App project in Visual Studio > Right-click on the AppName in the Solution Explorer > Select Add > Application Insights Telemetry.



5. Click the Get Started button
6. Select your account and subscription > Select the Existing resource you created in the Azure portal > Click Register.

References:
https://docs.microsoft.com/bs-latn-ba/azure/azure-monitor/learn/dotnetcore-quick-start?view=vs-2017

Question: 134

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. SourceGear Vault
B. Jenkins
C. Microsoft Visual SourceSafe
D. WhiteSource Bolt

Answer: D

Explanation:

WhiteSource provides WhiteSource Bolt, a lightweight open source security and management solution developed specifically for integration with Azure DevOps and Azure DevOps Server.

Note: 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.
Reference:
https://www.azuredevopslabs.com/labs/vstsextend/whitesource/

Question: 135

You are implementing an Azure DevOps strategy for mobile devices using App Center.
You plan to use distribution groups to control access to releases.
You need to create the distribution groups shown in the following table.

Name	Use
Group1	Application testers who are invited by email
Group2	Early release users who use unauthenticated public links
Group3	Application testers for all the apps of your company

Which type of distribution group should you use for each group? To answer, drag the appropriate group types to the correct locations. Each group type 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.

Answer:

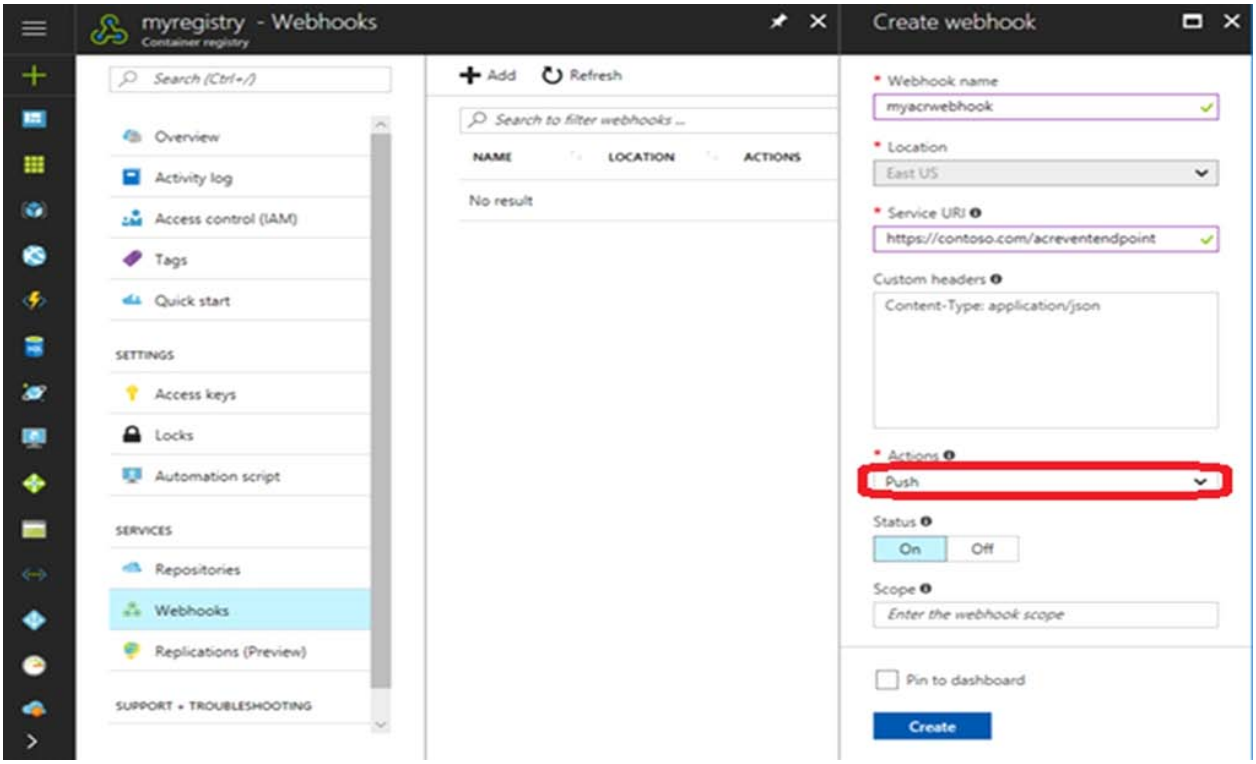
Explanation:
Box1: Private
In App Center, distribution groups are private by default. Only testers invited via email can access the releases available to this group.
Box 2: Public
Distribution groups must be public to enable unauthenticated installs from public links.
Box 3: Shared
Shared distribution groups are private or public distribution groups that are shared across multiple apps in a single organization.
Reference:
https://docs.microsoft.com/en-us/appcenter/distribution/groups

Question: 136

You need to ensure that the https://contoso.com/statushook webhook is called every time a repository named az40010480345acr1 receives a new version of an image named dotnetapp.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
Sign in to the Azure portal.
Navigate to the container registry az40010480345acr1.
Under Services, select Webhooks.
Select the existing webhook https://contoso.com/statushook, and double-click on it to get its properties.
For Trigger actions select image push
Example web hook:



Reference:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-webhook

Question: 137

You have an Azure DevOps project named Project1 and an Azure subscription named Sub1. Sub1 contains an Azure SQL database named DB1.
You need to create a release pipeline that uses the Azure SQL Database Deployment task to update DB1.
Which artifact should you deploy?

A. a BACPAC
B. a DACPAC
C. an LDF file
D. an MDF file

Answer: B

Explanation:
Use Azure SQL Database Deployment task in a build or release pipeline to deploy to Azure SQL DB using a DACPAC or run scripts using SQLCMD.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/deploy/sql-azure-dacpac-deployment

Question: 138

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 manage a project in Azure DevOps.
You need to prevent the configuration of the project from changing over time.
Solution: Add a code coverage step to the build pipelines.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead implement Continuous Assurance for the project.
Reference:
https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html

Question: 139

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 manage a project in Azure DevOps.
You need to prevent the configuration of the project from changing over time.
Solution: Implement Continuous Integration for the project.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead implement Continuous Assurance for the project.
Reference:
https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html

Question: 140

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 manage a project in Azure DevOps.
You need to prevent the configuration of the project from changing over time.
Solution: Implement Continuous Assurance for the project.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
The basic idea behind Continuous Assurance (CA) is to setup the ability to check for "drift" from what is considered a secure snapshot of a system. Support for Continuous Assurance lets us treat security truly as a 'state' as opposed to a 'point in time' achievement. This is particularly important in today's context when 'continuous change' has become a norm.
There can be two types of drift:
Drift involving 'baseline' configuration: This involves settings that have a fixed number of possible states (often pre-defined/statically determined ones). For instance, a SQL DB can have TDE encryption turned ON or OFF…or a Storage Account may have auditing turned ON however the log retention period may be less than 365 days.
Drift involving 'stateful' configuration: There are settings which cannot be constrained within a finite set of well-known states. For instance, the IP addresses configured to have access to a SQL DB can be any (arbitrary) set of IP addresses. In such scenarios, usually human judgment is initially required to determine whether a particular configuration should be considered 'secure' or not. However, once that is done, it is important to ensure that there is no "stateful drift" from the attested configuration. (E.g., if, in a troubleshooting session, someone adds the IP address of a developer machine to the list, the Continuous Assurance feature should be able to identify the drift and generate notifications/alerts or even trigger 'auto-remediation' depending on the severity of the change).
Reference:
https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html

Question: 141

Your company has a release pipeline in an Azure DevOps project.
You plan to deploy to an Azure Kubernetes Services (AKS) cluster by using the Helm package and deploy task.
You need to install a service in the AKS namespace for the planned deployment.
Which service should you install?

A. Azure Container Registry
B. Chart
C. Kubectl

D. Tiller

Answer: D

Explanation:
Before you can deploy Helm in an RBAC-enabled AKS cluster, you need a service account and role binding for the Tiller service.
Incorrect Answers:
C: Kubectl is a command line interface for running commands against Kubernetes clusters.
Reference:
https://docs.microsoft.com/en-us/azure/aks/kubernetes-helm

Question: 142

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 need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:
- The builds must access an on-premises dependency management system.
- The build outputs must be stored as Server artifacts in Azure DevOps.
- The source code must be stored in a Git repository in Azure DevOps.

Solution: Configure the build pipeline to use a Hosted Ubuntu agent pool. Include the Java Tool Installer task in the build pipeline. Does this meet the goal?

A. Yes
B. No

Answer: A

Question: 143

You plan to use a NuGet package in a project in Azure DevOps. The NuGet package is in a feed that requires authentication.
You need to ensure that the project can restore the NuGet package automatically.
What should the project use to automate the authentication?

A. an Azure Automation account
B. an Azure Artifacts Credential Provider
C. an Azure Active Directory (Azure AD) account that has multi-factor authentication (MFA) enabled
D. an Azure Active Directory (Azure AD) service principal
D18912E1457D5D1DDCBD40AB3BF70D5D

Answer: B

Explanation:
The Azure Artifacts Credential Provider automates the acquisition of credentials needed to restore NuGet
packages as part of your .NET development workflow. It integrates with MSBuild, dotnet, and NuGet(.exe) and works on Windows, Mac, and Linux. Any time you want to use packages from an Azure Artifacts feed, the Credential Provider will automatically acquire and securely store a token on behalf of the NuGet client you're using.
Reference:
https://github.com/Microsoft/artifacts-credprovider

Question: 144

You need to create deployment files for an Azure Kubernetes Service (AKS) cluster. The deployments must meet the provisioning storage requirements shown in the following table.

Deployment	Requirement
Deployment 1	Use files stored on an SMB-based share from the container's file system.
Deployment 2	Use files on a managed disk from the container's file system.
Deployment 3	Securely access X.509 certificates from the container's file system.

Which resource type should you use for each deployment? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Deployment 1:

- azurekeyvault-flexvolume
- blobfuse-flexvol
- kubernetes.io/azure-disk
- kubernetes.io/azure-file
- volume.beta.kubernetes.io/storage-provisioner

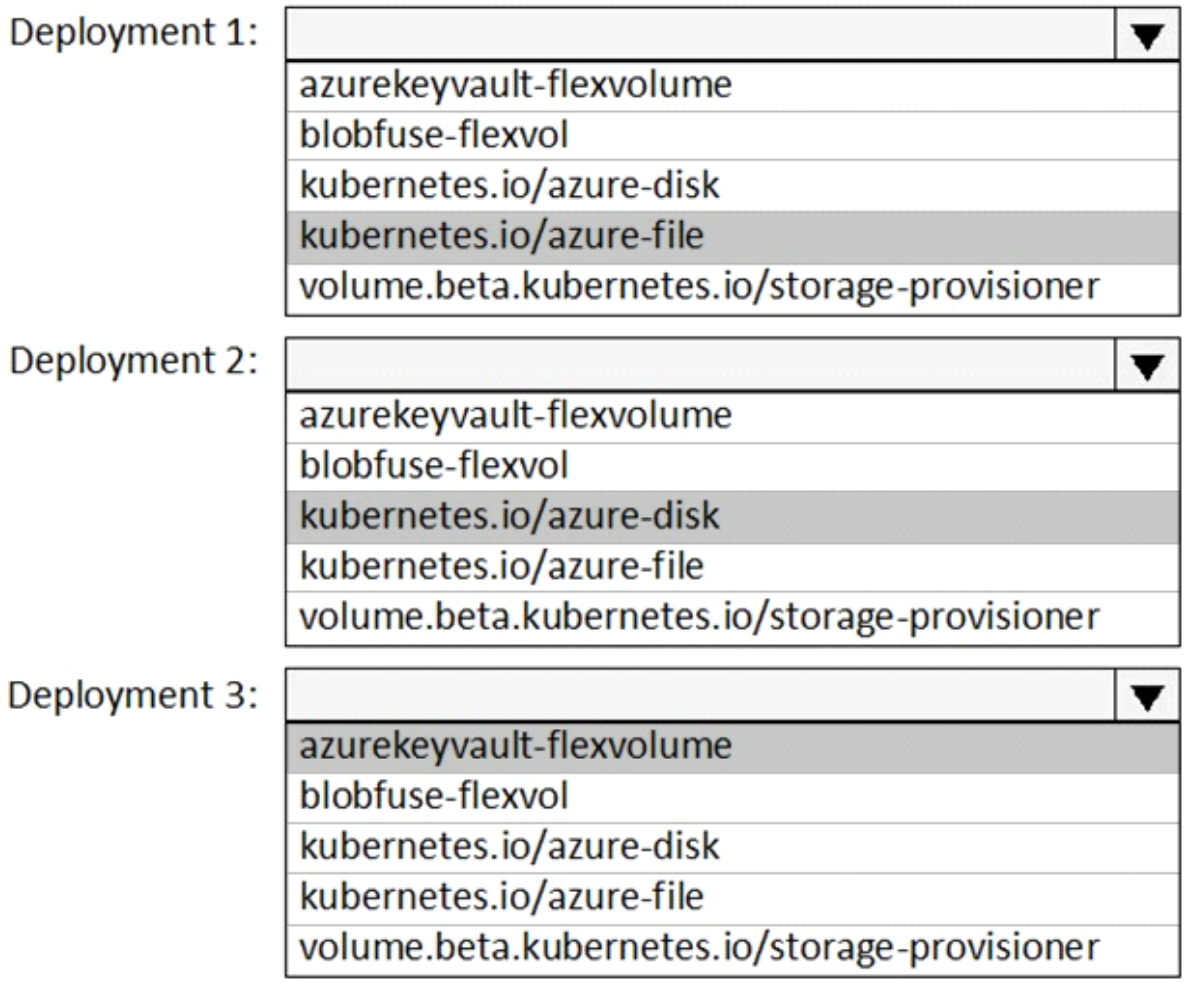
Deployment 2:

- azurekeyvault-flexvolume
- blobfuse-flexvol
- kubernetes.io/azure-disk
- kubernetes.io/azure-file
- volume.beta.kubernetes.io/storage-provisioner

Deployment 3:

- azurekeyvault-flexvolume
- blobfuse-flexvol
- kubernetes.io/azure-disk
- kubernetes.io/azure-file
- volume.beta.kubernetes.io/storage-provisioner

Answer:



Explanation:
Deployment 1: Kubernetes.io/azure-file
You can use Azure Files to connect using the Server Message Block (SMB) protocol.
Deployment 2: Kubernetes.io/azure-disk
Deployment 3: azurekeyvault-flexvolume
azurekeyvault-flexvolume: Key Vault FlexVolume: Seamlessly integrate your key management systems with Kubernetes.
Secrets, keys, and certificates in a key management system become a volume accessible to pods. Once the volume is mounted, its data is available directly in the container filesystem for your application.
Incorrect Answers:
blobfuse-flexvolume: This driver allows Kubernetes to access virtual filesystem backed by the Azure Blob storage.
References:
https://docs.microsoft.com/bs-cyrl-ba/azure/aks/azure-files-dynamic-pv
https://docs.microsoft.com/en-us/azure/aks/azure-disks-dynamic-pv

Question: 145

You create a Microsoft ASP.NET Core application.
You plan to use Azure Key Vault to provide secrets to the application as configuration data.

You need to create a Key Vault access policy to assign secret permissions to the application. The solution must use the principle of least privilege.
Which secret permissions should you use?

A. List only
B. Get only
C. Get and List

Answer: B

Explanation:
Application data plane permissions:
Keys: sign
Secrets: get
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

Question: 146

You need to deploy Azure Kubernetes Service (AKS) to host an application. The solution must meet the following requirements:
Containers must only be published internally.
AKS clusters must be able to create and manage containers in Azure.
What should you use for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Containers must only be published internally:

- Azure Container Instances
- Azure Container Registry
- Dockerfile

AKS clusters must be able to create and manage containers in Azure:

- An Azure Active Directory (Azure AD) group
- An Azure Automation account
- An Azure service principal

Answer:

Containers must only be published internally:	Azure Container Instances **Azure Container Registry** Dockerfile
AKS clusters must be able to create and manage containers in Azure:	An Azure Active Directory (Azure AD) group An Azure Automation account **An Azure service principal**

Explanation:
Box 1: Azure Container Registry
Azure services like Azure Container Registry (ACR) and Azure Container Instances (ACI) can be used and connected from independent container orchestrators like kubernetes (k8s). You can set up a custom ACR and connect it to an existing k8s cluster to ensure images will be pulled from the private container registry instead of the public docker hub.
Box 2: An Azure service principal
When you're using Azure Container Registry (ACR) with Azure Kubernetes Service (AKS), an authentication mechanism needs to be established. You can set up AKS and ACR integration during the initial creation of your AKS cluster. To allow an AKS cluster to interact with ACR, an Azure Active Directory service principal is used.
References:
https://thorsten-hans.com/how-to-use-private-azure-container-registry-with-kubernetes
https://docs.microsoft.com/en-us/azure/aks/cluster-container-registry-integration

Question: 147

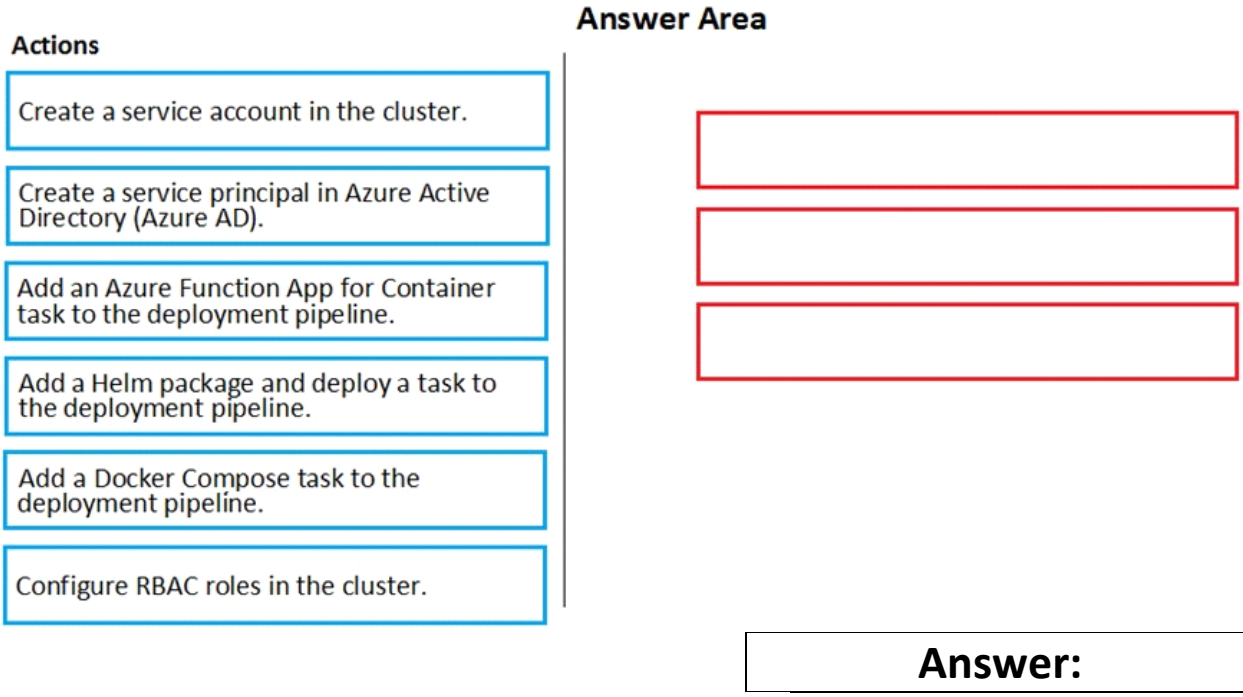
You are designing an Azure DevOps strategy for your company's development team.
You suspect that the team's productivity is low due to accumulate technical debt.
You need to recommend a metric to assess the amount of the team's technical debt.
What should you recommend?

A. the number of code modules in an application
B. the number of unit test failures
C. the percentage of unit test failures
D. the percentage of overall time spent on rework

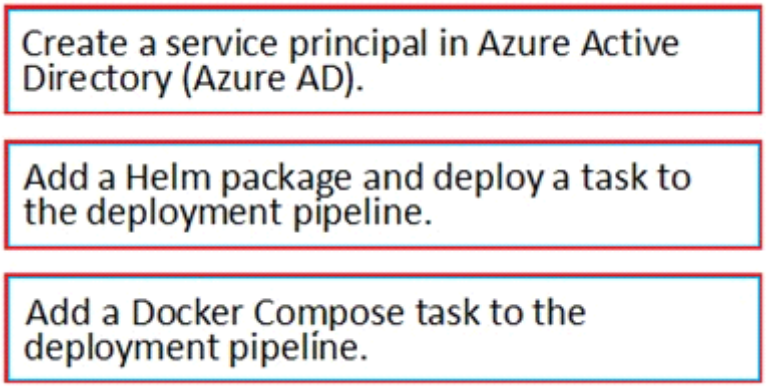
Answer: D

Question: 148

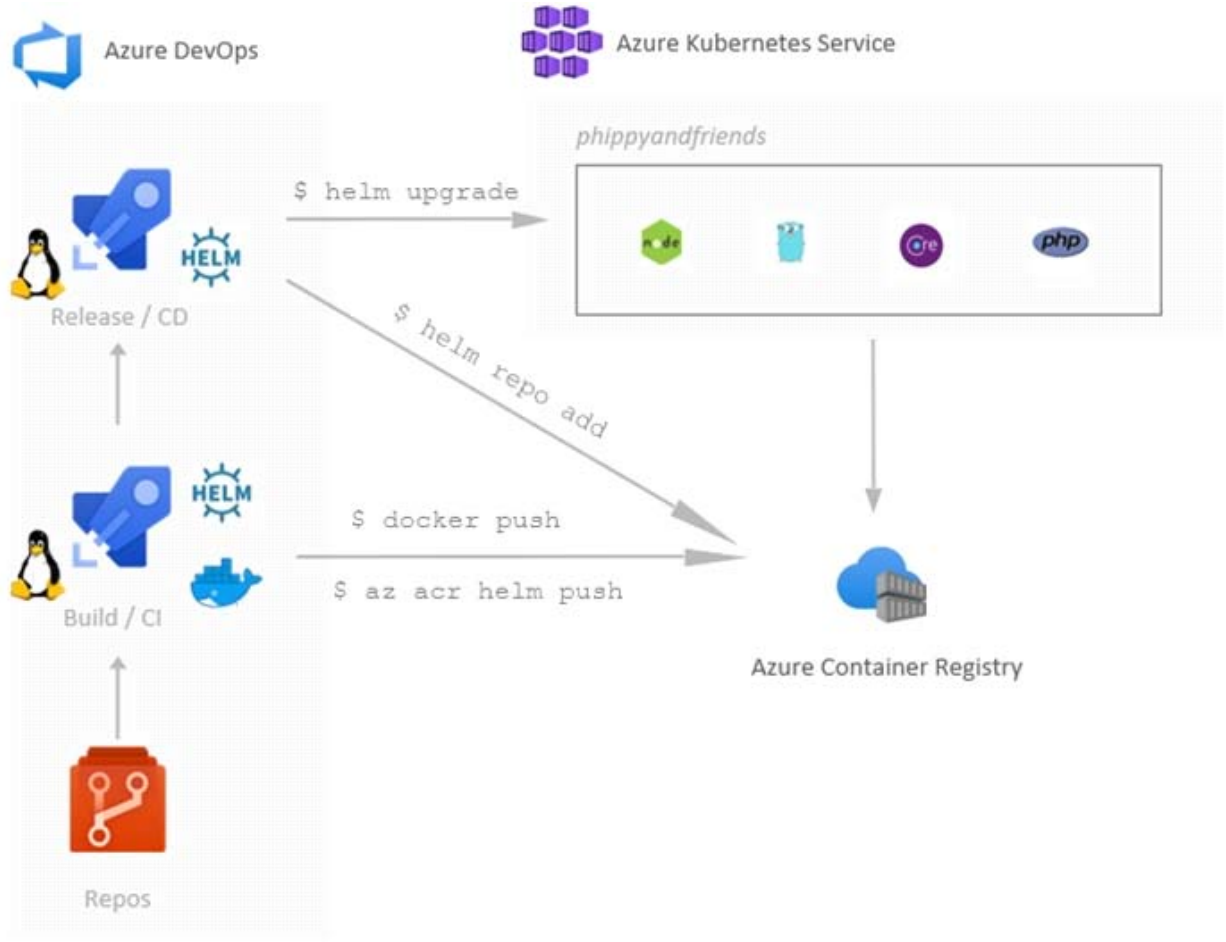
You have an Azure Kubernetes Service (AKS) cluster.
You need to deploy an application to the cluster by using Azure DevOps.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:
You can set up a CI/CD pipeline to deploy your apps on a Kubernetes cluster with Azure DevOps by leveraging a Linux agent, Docker, and Helm.
Step 1: Create a service principle in Azure Active Directory (Azure AD)
We need to assign 3 specific service principals with specific Azure Roles that need to interact with our ACR and our AKS.
Create a specific Service Principal for our Azure DevOps pipelines to be able to push and pull images and charts of our ACR.
Create a specific Service Principal for our Azure DevOps pipelines to be able to deploy our application in our AKS.
Step 2: Add a Helm package and deploy a task to the deployment pipeline
This is the DevOps workflow with containers:



Step 3: Add a Docker Compose task to the deployment pipeline.
Dockerfile file is a script leveraged by Docker, composed of various commands (instructions) and arguments listed successively to automatically perform actions on a base image in order to create a new Docker image by packaging the app.
Reference:
https://cloudblogs.microsoft.com/opensource/2018/11/27/tutorial-azure-devops-setup-cicd-pipeline-kubernetes-docker-helm/

Question: 149

You have an Azure DevOps project that contains a build pipeline. The build pipeline uses approximately 50 open source libraries.
You need to ensure that all the open source libraries comply with your company's licensing standards.
Which service should you use?

A. NuGet
B. Maven
C. Black Duck
D. Helm

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.
Reference:
https://marketplace.visualstudio.com/items?itemName=black-duck-software.hub-tfs

Question: 150

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 manage a project in Azure DevOps.
You need to prevent the configuration of the project from changing over time.
Solution: Perform a Subscription Health scan when packages are created.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead implement Continuous Assurance for the project.
Note: The Subscription Security health check features in AzSK contains a set of scripts that examines a subscription and flags off security issues, misconfigurations or obsolete artifacts/settings which can put your subscription at higher risk.
Reference:
https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html

Question: 151

You are developing an iOS application by using Azure DevOps.
You need to test the application manually on 10 devices without releasing the application to the public.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Create a Microsoft Intune device compliance policy.

B. Deploy a certificate from an internal certification authority (CA) to each device.
C. Register the application in the iTunes store.
D. Onboard the devices into Microsoft Intune.
E. Distribute a new release of the application.
F. Register the IDs of the devices in the Apple Developer portal.

Answer: BF

References:
https://docs.microsoft.com/en-us/appcenter/distribution/auto-provisioning

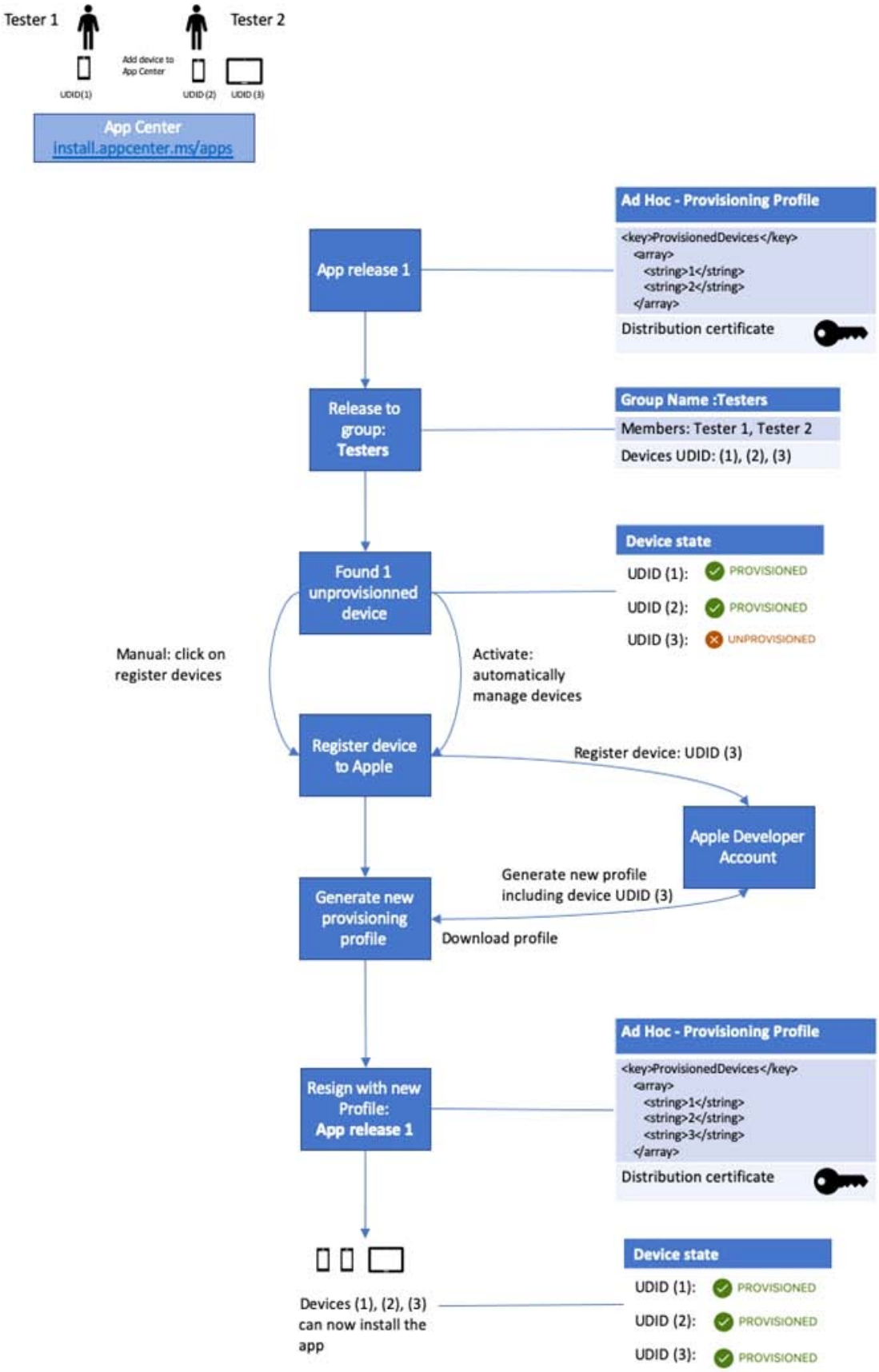
Question: 152

You have a private distribution group that contains provisioned and unprovisioned devices.
You need to distribute a new iOS application to the distribution group by using Microsoft Visual Studio App Center.
What should you do?

A. Select Register devices and sign my app.
B. Generate a new .p12 file for each device.
C. Create an active subscription in App Center Test.
D. Add the device owner to the collaborators group.

Answer: A

Explanation:
The following diagram displays the entire app re-signing flow in App Center.


Tester 1
Tester 2
Add device to App Center
UDID(1)
UDID (2)
UDID (3)
App Center
install.appcenter.ms/apps
Ad Hoc - Provisioning Profile
<key>ProvisionedDevices</key>
<array>
<string>1</string>
<string>2</string>
</array>
Distribution certificate
App release 1
Release to group: Testers
Group Name :Testers
Members: Tester 1, Tester 2
Devices UDID: (1), (2), (3)
Device state
UDID (1): PROVISIONED
UDID (2): PROVISIONED
UDID (3): UNPROVISIONED
Found 1 unprovisionned device
Manual: click on register devices
Activate: automatically manage devices
Register device to Apple
Register device: UDID (3)
Apple Developer Account
Generate new profile including device UDID (3)
Generate new provisioning profile
Download profile
Ad Hoc - Provisioning Profile
<key>ProvisionedDevices</key>
<array>
<string>1</string>
<string>2</string>
<string>3</string>
</array>
Distribution certificate
Resign with new Profile: App release 1
Devices (1), (2), (3) can now install the app
Device state
UDID (1): PROVISIONED
UDID (2): PROVISIONED
UDID (3): PROVISIONED

Incorrect Answers:
B: Only one .p12 file for the app, not one for each device.
Reference:
https://docs.microsoft.com/hu-hu/appcenter/distribution/auto-provisioning

Question: 153

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.
The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.
You need to recommend changes to reduce the accumulated technical debt.
Solution: You recommend increasing the code duplication.
Does this meet the goal?

A. Yes
B. No

Answer: B

Instead reduce the code complexity.
Reference:
https://dzone.com/articles/fight-through-the-pain-how-to-deal-with-technical

Question: 154

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.
The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.
You need to recommend changes to reduce the accumulated technical debt.
Solution: You recommend increasing the test coverage.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Instead reduce the code complexity.
Reference:
https://dzone.com/articles/fight-through-the-pain-how-to-deal-with-technical

Question: 155

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.
The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.
You need to recommend changes to reduce the accumulated technical debt.
Solution: You recommend reducing the code complexity.
Does this meet the goal?

A. Yes
B. No

Answer: A

Reference:
https://dzone.com/articles/fight-through-the-pain-how-to-deal-with-technical

Question: 156

Your company has 60 developers who are assigned to four teams. Each team has 15 members.
The company uses an agile development methodology.
You need to structure the work of the development teams so that each team owns their respective work while working together to reach a common goal.
Which parts of the taxonomy should you enable the team to perform autonomously?

A. Features and Tasks
B. Initiatives and Epics
C. Epics and Features
D. Stories and Tasks

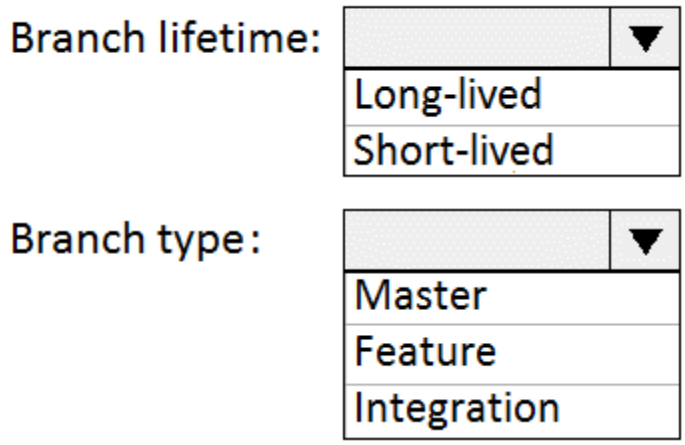
Answer: A

Explanation:
A feature typically represents a shippable component of software.
Features, examples:
Add view options to the new work hub
Add mobile shopping cart
Support text alerts

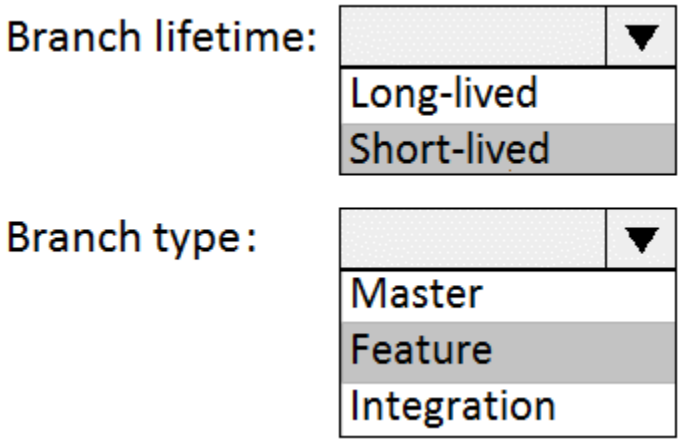
Refresh the web portal with new look and feel
User Stories and Tasks are used to track work. Teams can choose how they track bugs, either as requirements or as tasks
Reference:
https://docs.microsoft.com/en-us/azure/devops/boards/backlogs/define-features-epics
https://docs.microsoft.com/en-us/azure/devops/boards/work-items/about-work-items

Question: 157

Your company uses Git as a source code control system for a complex app named App1.
You plan to add a new functionality to App1.
You need to design a branching model for the new functionality.
Which branch lifetime and branch time should you use in the branching model? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
Branch lifetime: Short-lived
Branch type: Feature

Feature branches are used when developing a new feature or enhancement which has the potential of a development lifespan longer than a single deployment. When starting development, the deployment in which this feature will be released may not be known. No matter when the feature branch will be finished, it will always be merged back into the master branch.
References:
https://gist.github.com/digitaljhelms/4287848

Question: 158

You store source code in a Git repository in Azure repos. You use a third-party continuous integration (CI) tool to control builds.
What will Azure DevOps use to authenticate with the tool?

A. certificate authentication
B. a personal access token (PAT)
C. a Shared Access Signature (SAS) token
D. NTLM authentication

Answer: B

Explanation:
Personal access tokens (PATs) give you access to Azure DevOps and Team Foundation Server (TFS), without using your username and password directly.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/auth-overview

Question: 159

Your company creates a new Azure DevOps team.
D18912E1457D5D1DDCBD40AB3BF70D5D
You plan to use Azure DevOps for sprint planning.
You need to visualize the flow of your work by using an agile methodology.
Which Azure DevOps component should you use?

A. Kanban boards
B. sprint planning
C. delivery plans
D. portfolio backlogs

Answer: A

Explanation:
Customizing Kanban boards
To maximize a team's ability to consistently deliver high quality software, Kanban emphasize two main practices. The first, visualize the flow of work, requires you to map your team's workflow stages and configure your Kanban board to match. Your Kanban board turns your backlog into an interactive signboard, providing a visual flow of work.

Reference:
https://azuredevopslabs.com/labs/azuredevops/agile/

Question: 160

You are deploying a server application that will run on a Server Core installation of Windows Server 2019.
You create an Azure key vault and a secret.
You need to use the key vault to secure API secrets for third-party integrations.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
D18912E1457D5D1DDCBD40AB3BF70D5D

A. Configure RBAC for the key vault.
B. Modify the application to access the key vault.
C. Configure a Key Vault access policy.
D. Deploy an Azure Desired State Configuration (DSC) extension.
E. Deploy a virtual machine that uses a system-assigned managed identity.

Answer: BCE

Explanation:
BE: An app deployed to Azure can take advantage of Managed identities for Azure resources, which allows the app to authenticate with Azure Key Vault using Azure AD authentication without credentials (Application ID and Password/Client Secret) stored in the app.
Select Add Access Policy.
Open Secret permissions and provide the app with Get and List permissions.
Select Select principal and select the registered app by name. Select the Select button.
Select OK.
Select Save.
Deploy the app.
References:
https://docs.microsoft.com/en-us/aspnet/core/security/key-vault-configuration

Question: 161

You manage build and release pipelines by using Azure DevOps. Your entire managed environment resides in Azure.
You need to configure a service endpoint for accessing Azure Key Vault secrets. The solution must meet the following requirements:
Ensure that the secrets are retrieved by Azure DevOps.
Avoid persisting credentials and tokens in Azure DevOps.
How should you configure the service endpoint? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Service connection type:

- Azure Resource Manager
- Generic service
- Team Foundation Server / Azure Pipelines service connection

Authentication/authorization method for the connection:

- Azure Active Directory OAuth 2.0
- Grant authorization
- Managed Service Identity Authentication

Answer:

Service connection type:

- Azure Resource Manager
- Generic service
- Team Foundation Server / Azure Pipelines service connection

Authentication/authorization method for the connection:

- Azure Active Directory OAuth 2.0
- Grant authorization
- Managed Service Identity Authentication

Explanation:
Box 1: Azure Pipelines service connection
Box 2: Managed Service Identity Authentication
The managed identities for Azure resources feature in Azure Active Directory (Azure AD) provides Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/deploy/azure-key-vault
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

Question: 162

Your company has an Azure subscription named Subscription1. Subscription1 is associated to an Azure Active Directory tenant named contoso.com.
You need to provision an Azure Kubernetes Services (AKS) cluster in Subscription1 and set the permissions for the cluster by using RBAC roles that reference the identities in contoso.com.
Which three objects should you create in sequence? To answer, move the appropriate objects from the list of objects to the answer area and arrange them in the correct order.

Answer Area

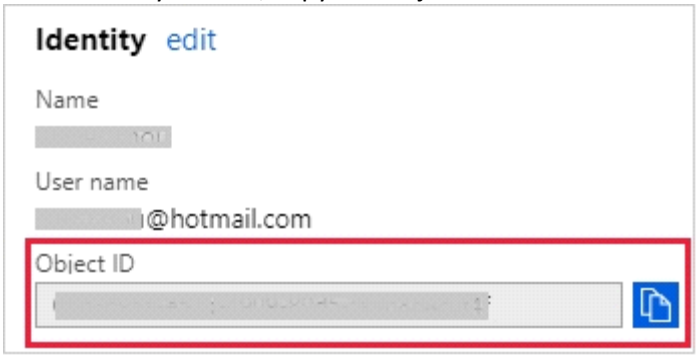
Objects

- a system-assigned managed identity
- a cluster
- an application registration in contoso.com
- an RBAC binding

Answer:

- a cluster
- a system-assigned managed identity
- an RBAC binding

Explanation:
Step 1: Create an AKS cluster
Step 2: a system-assigned managed identity
To create an RBAC binding, you first need to get the Azure AD Object ID.
Sign in to the Azure portal.
In the search field at the top of the page, enter Azure Active Directory.
Click Enter.
In the Manage menu, select Users.
In the name field, search for your account.
In the Name column, select the link to your account.
In the Identity section, copy the Object ID.

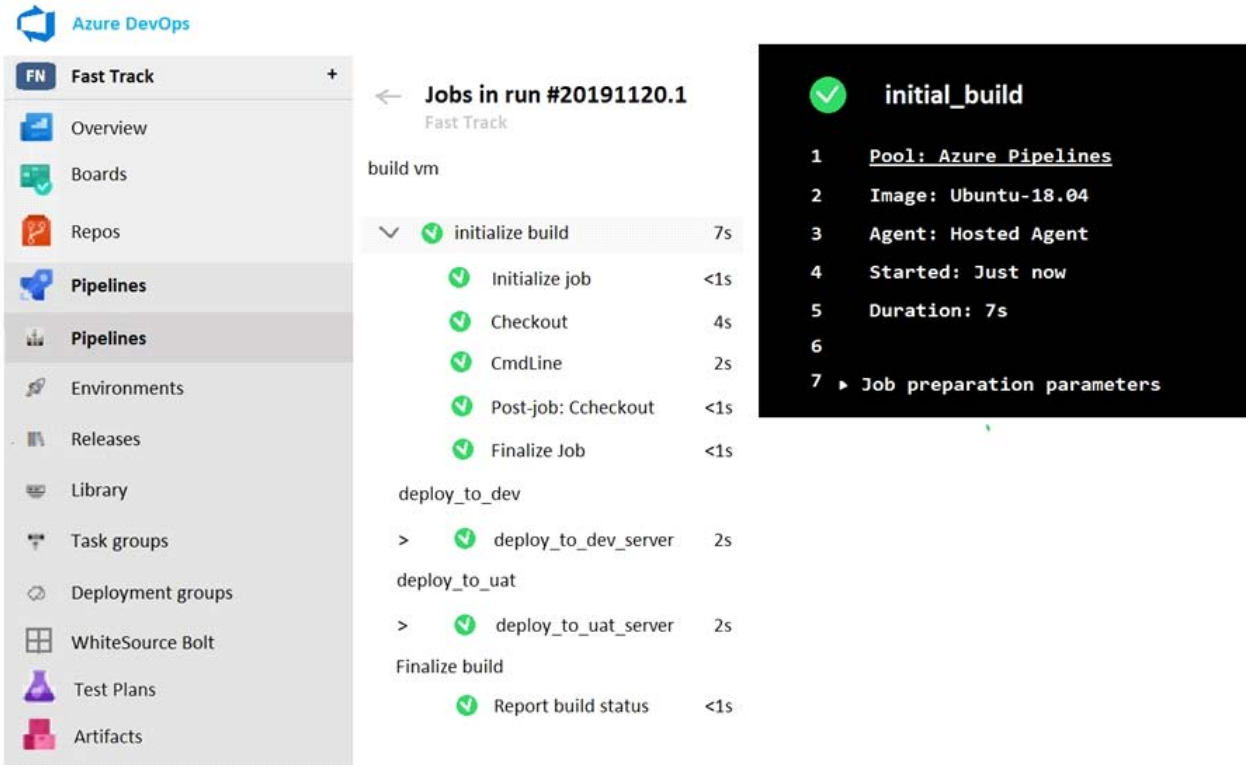


Step 3: a RBAC binding

Reference:
https://docs.microsoft.com/en-us/azure/developer/ansible/aks-configure-rbac

Question: 163

You company uses Azure DevOps to deploy infrastructures to Azure.
Pipelines are developed by using YAML.
You execute a pipeline and receive the results in the web portal for Azure Pipelines as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

The pipeline contains

- one stage
- two stages
- three stages
- four stages
- five stages

Build_vm contains

- one job
- two jobs
- three jobs
- four jobs
- five jobs

Answer:

The pipeline contains

- one stage
- two stages
- three stages
- four stages
- five stages

Build_vm contains

- one job
- two jobs
- three jobs
- four jobs
- five jobs

Reference:
https://dev.to/rajikaimal/azure-devops-ci-cd-yaml-pipeline-4glj

Question: 164

You need to ensure that Microsoft Visual Studio 2017 can remotely attach to an Azure Function named fa-11566895.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

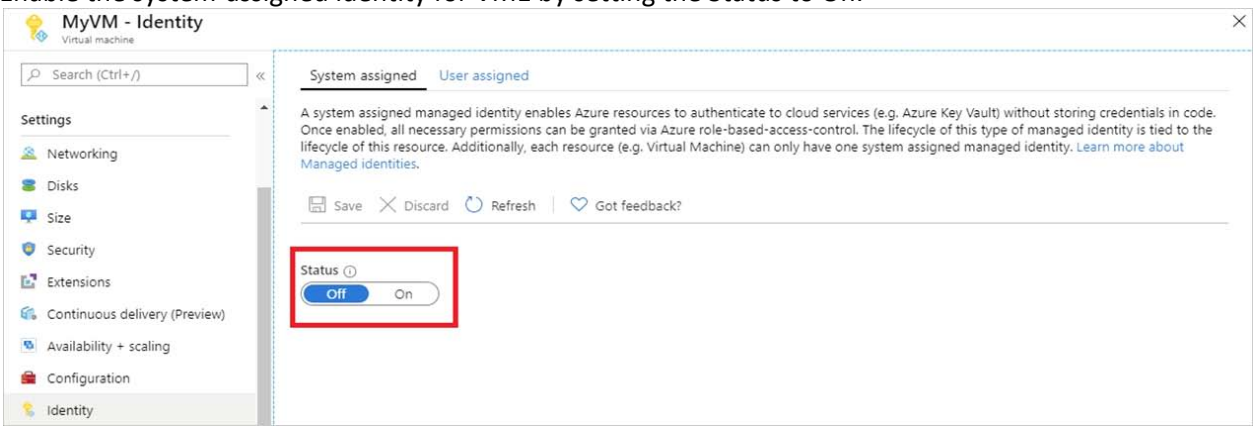
Explanation:
Enable Remote Debugging
Before we start a debugging session to our Azure Function app we need to enable the functionality.
Navigate in the Azure portal to your function app fa-11566895
Go to the "Application settings"
Under "Debugging" set Remote Debugging to On and set Remote Visual Studio version to 2017.
Reference:
https://www.locktar.nl/uncategorized/azure-remote-debugging-manually-in-visual-studio-2017/

Question: 165

You need to configure a virtual machine named VM1 to securely access stored secrets in an Azure Key Vault named az400-11566895-kv.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
You can use a system-assigned managed identity for a Windows virtual machine (VM) to access Azure Key Vault.
Sign in to Azure portal
Locate virtual machine VM1.
Select Identity
Enable the system-assigned identity for VM1 by setting the Status to On.



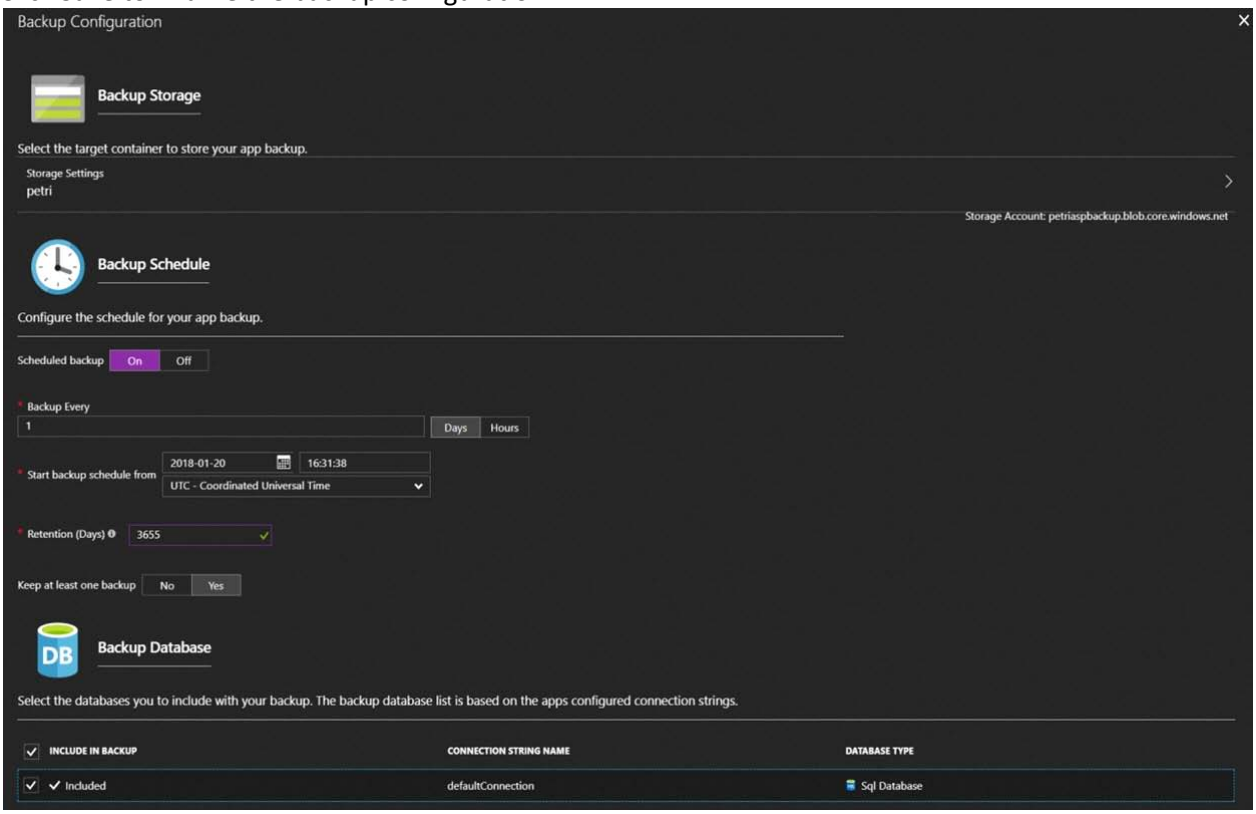
Note: Enabling a system-assigned managed identity is a one-click experience. You can either enable it during the creation of a VM or in the properties of an existing VM.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad

Question: 166

Your company plans to implement a new compliance strategy that will require all Azure web apps to be backed up every five hours.
You need to back up an Azure web app named az400-11566895-main every five hours to an Azure Storage account in your resource group.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
With the storage account ready, you can configure backs up in the web app or App Service.
Open the App Service az400-11566895-main, which you want to protect, in the Azure Portal and browse to Settings > Backups. Click Configure and a Backup Configuration blade should appear.
Select the storage account.
Click + to create a private container. You could name this container after the web app or App Service.
Select the container.
If you want to schedule backups, then set Scheduled Backup to On and configure a schedule: every five hours
Select your retention. Note that 0 means never delete backups.
Decide if at least one backup should always be retained.
Choose if any connected databases should be included in the web app backup.
Click Save to finalize the backup configuration.



Reference:
https://petri.com/backing-azure-app-service

Question: 167

You use WhiteSource Bolt to scan a Node.js application.
The WhiteSource Bolt scan identifies numerous libraries that have invalid licenses. The libraries are used only during development and are not part of a production deployment.
You need to ensure that WhiteSource Bolt only scans production dependencies.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Run npm install and specify the --production flag.
B. Modify the WhiteSource Bolt policy and set the action for the licenses used by the development tools to Reassign.
C. Modify the devDependencies section of the project's Package.json file.
D. Configure WhiteSource Bolt to scan the node_modules directory only.

Answer: AC

Explanation:
A: To resolve NPM dependencies, you should first run "npm install" command on the relevant folders before executing the plugin.
C: All npm packages contain a file, usually in the project root, called package.json - this file holds various metadata relevant to the project. This file is used to give information to npm that allows it to identify the project as well as handle the project's dependencies. It can also contain other metadata such as a project description, the version of the project in a particular distribution, license information, even configuration data - all of which can be vital to both npm and to the end users of the package.
Reference:
https://whitesource.atlassian.net/wiki/spaces/WD/pages/34209870/NPM+Plugin
https://nodejs.org/en/knowledge/getting-started/npm/what-is-the-file-package-json

Question: 168

You plan to deploy a runbook that will create Azure AD user accounts.
You need to ensure that runbooks can run the Azure PowerShell cmdlets for Azure Active Directory.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
Azure Automation now ships with the Azure PowerShell module of version 0.8.6, which introduced the ability to non-interactively authenticate to Azure using OrgId (Azure Active Directory user) credential-based authentication. Using the steps below, you can set up Azure Automation to talk to Azure using this authentication type.
Step 1: Find the Azure Active Directory associated with the Azure subscription to manage:
1. Log in to the Azure portal as the service administrator for the Azure subscription you want to manage using Azure Automation. You can find this user by logging in to the Azure portal as any user with access to this Azure subscription, then clicking Settings, then Administrators.

2. Note the name of the directory associated with the Azure subscription you want to manage. You can find this directory by clicking Settings, then Subscriptions.

Step 2: Create an Azure Active Directory user in the directory associated with the Azure subscription to manage:

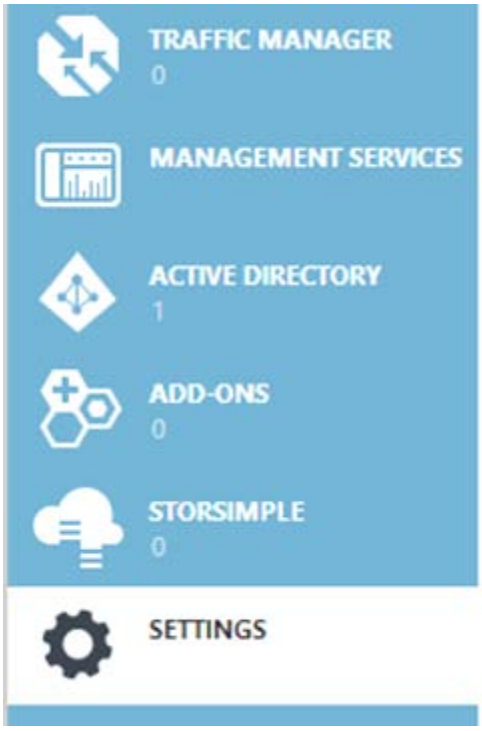
You can skip this step if you already have an Azure Active Directory user in this directory. and plan to use this OrgId to manage Azure.

1. In the Azure portal click on Active Directory service.

2. Click the directory name that is associated with this Azure subscription.
3. Click on the Users tab and then click the Add User button.
4. For type of user, select “New user in your organization.” Enter a username for the user to create.
5. Fill out the user’s profile. For role, pick “User.” Don’t enable multi-factor authentication. Multi-factor accounts cannot be used with Azure Automation.
6. Click Create.
7. Jot down the full username (including part after @ symbol) and temporary password.

Step 3: Allow this Azure Active Directory user to manage this Azure subscription.

1. Click on Settings (bottom Azure tab under StorSimple)

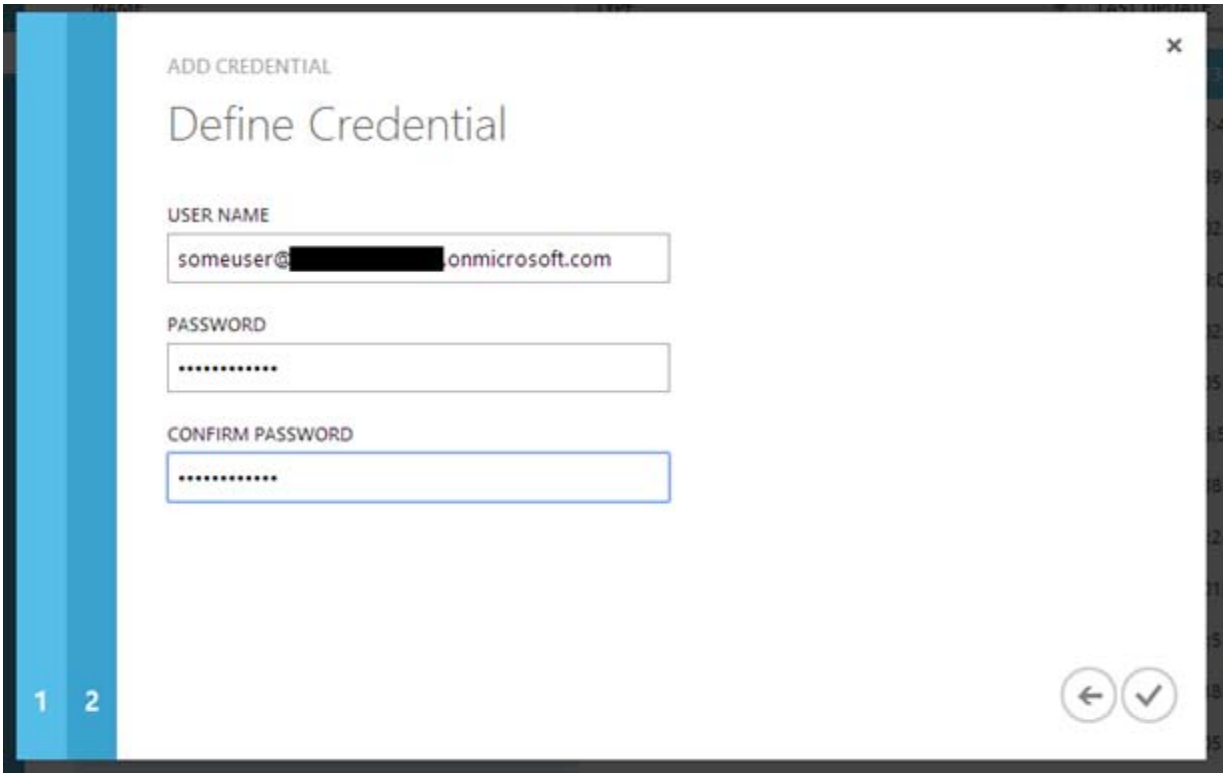


2. Click Administrators

3. Click the Add button. Type the full user name (including part after @ symbol) of the Azure Active Directory user you want to set up to manage Azure. For subscriptions, choose the Azure subscriptions you want this user to be able to manage. Click the check mark.

Step 4: Configure Azure Automation to use this Azure Active Directory user to manage this Azure subscription

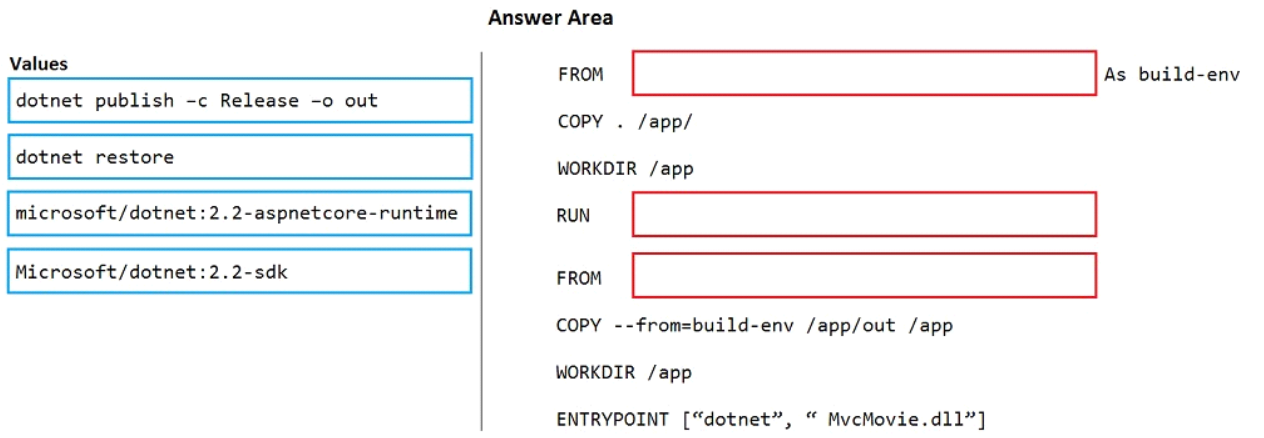
Create an Azure Automation credential asset containing the username and password of the Azure Active Directory user that you have just created. You can create a credential asset in Azure Automation by clicking into an Automation Account and then clicking the Assets tab, then the Add Setting button.



Note: Once you have set up the Azure Active Directory credential in Azure and Azure Automation, you can now manage Azure from Azure Automation runbooks using this credential.
References:
https://azure.microsoft.com/sv-se/blog/azure-automation-authenticating-to-azure-using-azure-active-directory/

Question: 169

You are creating a container for an ASP.NET Core app.
You need to create a Dockerfile file to build the image. The solution must ensure that the size of the image is minimized.
How should you configure the file? To answer, drag the appropriate values to the correct targets. Each value must 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.



Answer:

```
FROM Microsoft/dotnet:2.2-sdk As build-env
COPY . /app/
WORKDIR /app
RUN dotnet restore
FROM microsoft/dotnet:2.2-aspnetcore-runtime
COPY --from=build-env /app/out /app
WORKDIR /app
ENTRYPOINT ["dotnet", " MvcMovie.dll"]
```

Explanation:

Box 1: microsoft.com/dotnet/sdk:2.3

The first group of lines declares from which base image we will use to build our container on top of. If the local system does not have this image already, then docker will automatically try and fetch it. The mcr.microsoft.com/dotnet/core/sdk:2.1 comes packaged with the .NET core 2.1 SDK installed, so it's up to the task of building ASP .NET core projects targeting version 2.1

Box 2: dotnet restore

The next instruction changes the working directory in our container to be /app, so all commands following this one execute under this context.

COPY *.csproj ./

RUN dotnet restore

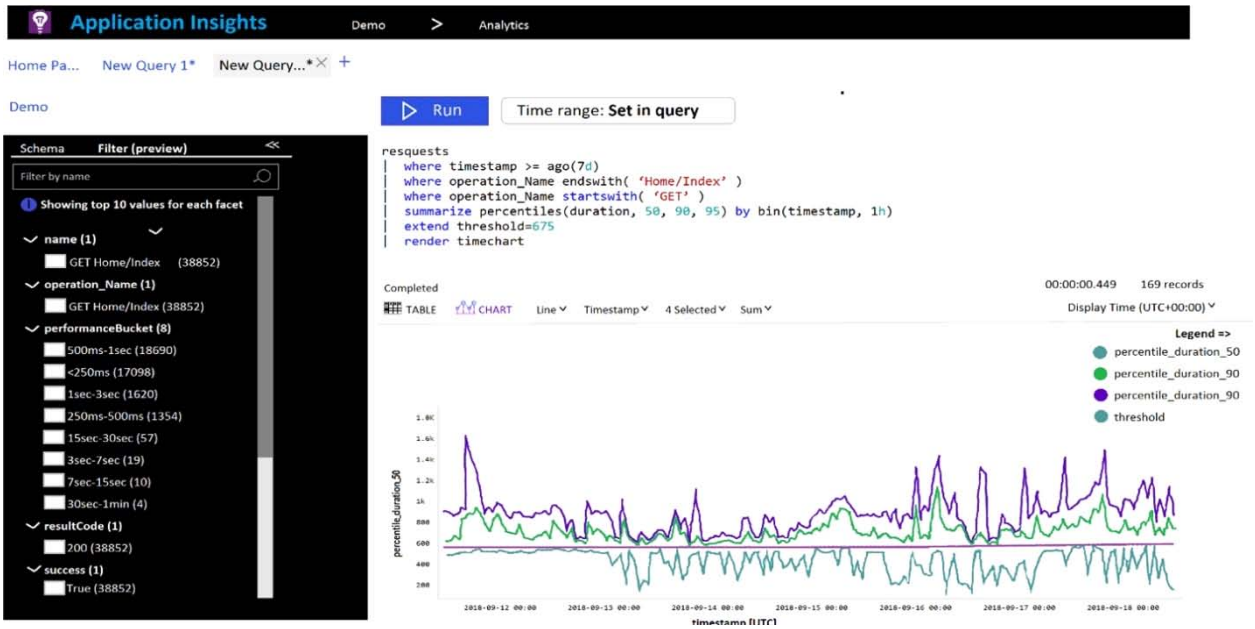
Box 3: microsoft.com/dotnet/2.2-aspnetcore-runtime

When building container images, it's good practice to include only the production payload and its dependencies in the container image. We don't want the .NET core SDK included in our final image

because we only need the .NET core runtime, so the dockerfile is written to use a temporary container that is packaged with the SDK called build-env to build the app.
Reference:
https://docs.microsoft.com/de-DE/virtualization/windowscontainers/quick-start/building-sample-app

Question: 170

You plan to create alerts that will be triggered based on the page load performance of a home page.
You have the Application Insights log query shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

To create an alert based on the page load experience of most users, the alerting level must be based on **[answer choice]**.

- percentile_duration_50
- percentile_duration_90
- percentile_duration_95
- threshold

To only create an alert when authentication error occurs on the server, the query must be filtered on **[answer choice]**.

- item Type
- resultCode
- source
- success

Answer:

To create an alert based on the page load experience of most users, the alerting level must be based on **[answer choice].**

- percentile_duration_50
- percentile_duration_90
- **percentile_duration_95**
- threshold

To only create an alert when authentication error occurs on the server, the query must be filtered on **[answer choice].**

- item Type
- resultCode
- source
- **success**

Explanation:
Box 1: percentile_duration_95
Box 2: success
For example –
requests
| project name, url, success
| where success == "False"
This will return all the failed requests in my App Insights within the specified time range.
Reference:
https://devblogs.microsoft.com/premier-developer/alerts-based-on-analytics-query-using-custom-log-search/

Question: 171

You are configuring the settings of a new Git repository in Azure Repos.
You need to ensure that pull requests in a branch meet the following criteria before they are merged:
Committed code must compile successfully.
Pull requests must have a Quality Gate status of Passed in SonarCloud.
Which policy type should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. Each policy type 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.

Policy Types

- A build policy
- A check-in policy
- A status policy

Committed code must compile successfully: [ ]

Pull requests must have a Quality Gate status of Passed in SonarCloud: [ ]

Answer:

Committed code must compile successfully:	A check-in policy
Pull requests must have a Quality Gate status of Passed in SonarCloud:	A build policy

Explanation:
Box 1: A check-in policy
Administrators of Team Foundation version control can add check-in policy requirements. These check-in policies require the user to take actions when they conduct a check-in to source control.
By default, the following check-in policy types are available:
Builds Requires that the last build was successful before a check-in.
Code Analysis Requires that code analysis is run before check-in.
Work Items Requires that one or more work items be associated with the check-in.
Box 2: Build policy
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/add-check-policies
https://azuredevopslabs.com/labs/vstsextend/sonarcloud/

Question: 172

You use a Git repository in Azure Repos to manage the source code of a web application. Developers commit changes directly to the master branch.
You need to implement a change management procedure that meets the following requirements:
The master branch must be protected, and new changes must be built in the feature branches first.
Changes must be reviewed and approved by at least one release manager before each merge.
Changes must be brought into the master branch by using pull requests.
What should you configure in Azure Repos?
D18912E1457D5D1DDCBD40AB3BF70D5D

A. branch policies of the master branch
B. Services in Project Settings
C. Deployment pools in Project Settings
D. branch security of the master branch

Answer: A

Branch policies help teams protect their important branches of development. Policies enforce your team's
code quality and change management standards.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

Question: 173

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 update the Azure DevOps strategy of your company.
You need to identify the following issues as they occur during the company's development process:
Licensing violations
Prohibited libraries
Solution: You implement continuous integration.
Does this meet the goal?

A. Yes
B. No

Answer: A

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.
Reference:
https://azuredevopslabs.com/labs/vstsextend/whitesource/

Question: 174

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 update the Azure DevOps strategy of your company.
You need to identify the following issues as they occur during the company's development process:
Licensing violations
Prohibited libraries
Solution: You implement pre-deployment gates.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Instead use implement continuous integration.
Note: 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.
Reference:
https://azuredevopslabs.com/labs/vstsextend/whitesource/

Question: 175

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 update the Azure DevOps strategy of your company.
You need to identify the following issues as they occur during the company's development process:
Licensing violations
Prohibited libraries
Solution: You implement automated security testing.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use implement continuous integration.
Note: 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.
Reference:
https://azuredevopslabs.com/labs/vstsextend/whitesource/

Question: 176

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 uses Azure DevOps to manage the build and release processes for applications.

You use a Git repository for applications source control.
You need to implement a pull request strategy that reduces the history volume in the master branch.
Solution: You implement a pull request strategy that uses fast-forward merges.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
No fast-forward merge - This option merges the commit history of the source branch when the pull request closes and creates a merge commit in the target branch.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

Question: 177

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 uses Azure DevOps to manage the build and release processes for applications.
You use a Git repository for applications source control.
You need to implement a pull request strategy that reduces the history volume in the master branch.
Solution: You implement a pull request strategy that uses squash merges.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use fast-forward merge.
Note:
Squash merge - Complete all pull requests with a squash merge, creating a single commit in the target branch with the changes from the source branch.
No fast-forward merge - This option merges the commit history of the source branch when the pull request closes and creates a merge commit in the target branch.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

Question: 178

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 uses Azure DevOps to manage the build and release processes for applications.
You use a Git repository for applications source control.
You need to implement a pull request strategy that reduces the history volume in the master branch.
Solution: You implement a pull request strategy that uses an explicit merge.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use fast-forward merge.
Note:
No fast-forward merge - This option merges the commit history of the source branch when the pull request closes and creates a merge commit in the target branch.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

Question: 179

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 uses Azure DevOps to manage the build and release processes for applications.
You use a Git repository for applications source control.
You need to implement a pull request strategy that reduces the history volume in the master branch.
Solution: You implement a pull request strategy that uses a three-way merge.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use fast-forward merge.
Note:

No fast-forward merge - This option merges the commit history of the source branch when the pull request closes and creates a merge commit in the target branch.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

Question: 180

You are developing an application. The application source has multiple branches.
You make several changes to a branch used for experimentation.
You need to update the main branch to capture the changes made to the experimentation branch and override the history of the Git repository.
Which Git option should you use?

A. Rebase
B. Fetch
C. Merge
D18912E1457D5D1DDCBD40AB3BF70D5D
D. Push

Answer: C

Explanation:
Create pull requests to review and merge code in a Git project. Pull requests let your team review code and give feedback on changes before merging it into the master branch.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/pull-requests

Question: 181

Your company plans to deploy an application to the following endpoints:
Ten virtual machines hosted in Azure
Ten virtual machines hosted in an on-premises data center environment
All the virtual machines have the Azure Pipelines agent.
You need to implement a release strategy for deploying the application to the endpoints.
What should you recommend using to deploy the application to the endpoints? To answer, drag the appropriate components to the correct endpoints. Each component 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.

Components	Answer Area
A deployment group	
A management group	Ten virtual machines hosted in Azure:
A resource group	Ten virtual machines hosted in an on-premises data center environment:
Application roles	

Answer:

Ten virtual machines hosted in Azure:	A deployment group
Ten virtual machines hosted in an on-premises data center environment:	A deployment group

Explanation:
Box 1: A deployment group
When authoring an Azure Pipelines or TFS Release pipeline, you can specify the deployment targets for a job using a deployment group.
If the target machines are Azure VMs, you can quickly and easily prepare them by installing the Azure Pipelines Agent Azure VM extension on each of the VMs, or by using the Azure Resource Group Deployment task in your release pipeline to create a deployment group dynamically.
Box 2: A deployment group
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deployment-groups

Question: 182

You plan to use Terraform to deploy an Azure resource group.
You need to install the required frameworks to support the planned deployment.
Which two frameworks should you install? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Vault
B. Terratest
C. Node.js
D. Yeoman
E. Tiller

Answer: BD

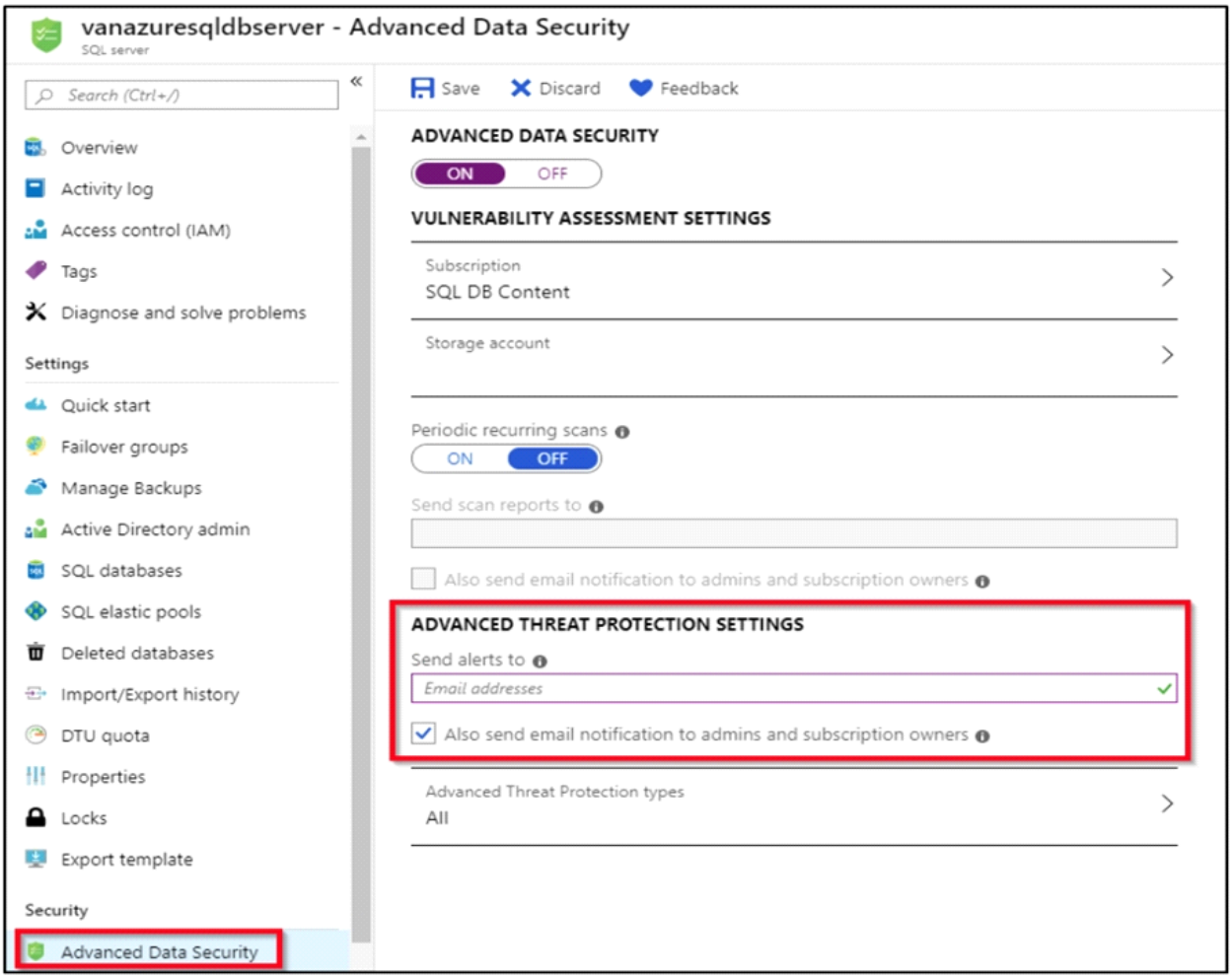
Explanation:
You can use the combination of Terraform and Yeoman. Terraform is a tool for creating infrastructure on Azure. Yeoman makes it easy to create Terraform modules.
Terratest provides a collection of helper functions and patterns for common infrastructure testing tasks, like making HTTP requests and using SSH to access a specific virtual machine. The following list describes some of the major advantages of using Terratest:
Convenient helpers to check infrastructure - This feature is useful when you want to verify your real infrastructure in the real environment.
Organized folder structure - Your test cases are organized clearly and follow the standard Terraform module folder structure.
Test cases are written in Go - Many developers who use Terraform are Go developers. If you're a Go developer, you don't have to learn another programming language to use Terratest.
Extensible infrastructure - You can extend additional functions on top of Terratest, including Azure-specific features.
Reference:
https://docs.microsoft.com/en-us/azure/developer/terraform/create-base-template-using-yeoman
https://docs.microsoft.com/en-us/azure/developer/terraform/test-modules-using-terratest

Question: 183

You manage a website that uses an Azure SQL Database named db1 in a resource group named RG1lod11566895.
You need to modify the SQL database to protect against SQL injection.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
Set up Advanced Threat Protection in the Azure portal
1. Sign into the Azure portal.
2. Navigate to the configuration page of the server you want to protect. In the security settings, select Advanced Data Security.
3. On the Advanced Data Security configuration page:



4. Enable Advanced Data Security on the server.

Note: Advanced Threat Protection for Azure SQL Database detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases. Advanced Threat Protection can identify Potential SQL injection, Access from unusual location or data center, Access from unfamiliar principal or potentially harmful application, and Brute force SQL credentials

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-account-create

https://docs.microsoft.com/en-us/azure/azure-sql/database/threat-detection-configure

Question: 184

You plan to implement a CI/CD strategy for an Azure Web App named az400-11566895-main.

You need to configure a staging environment for az400-11566895-main.

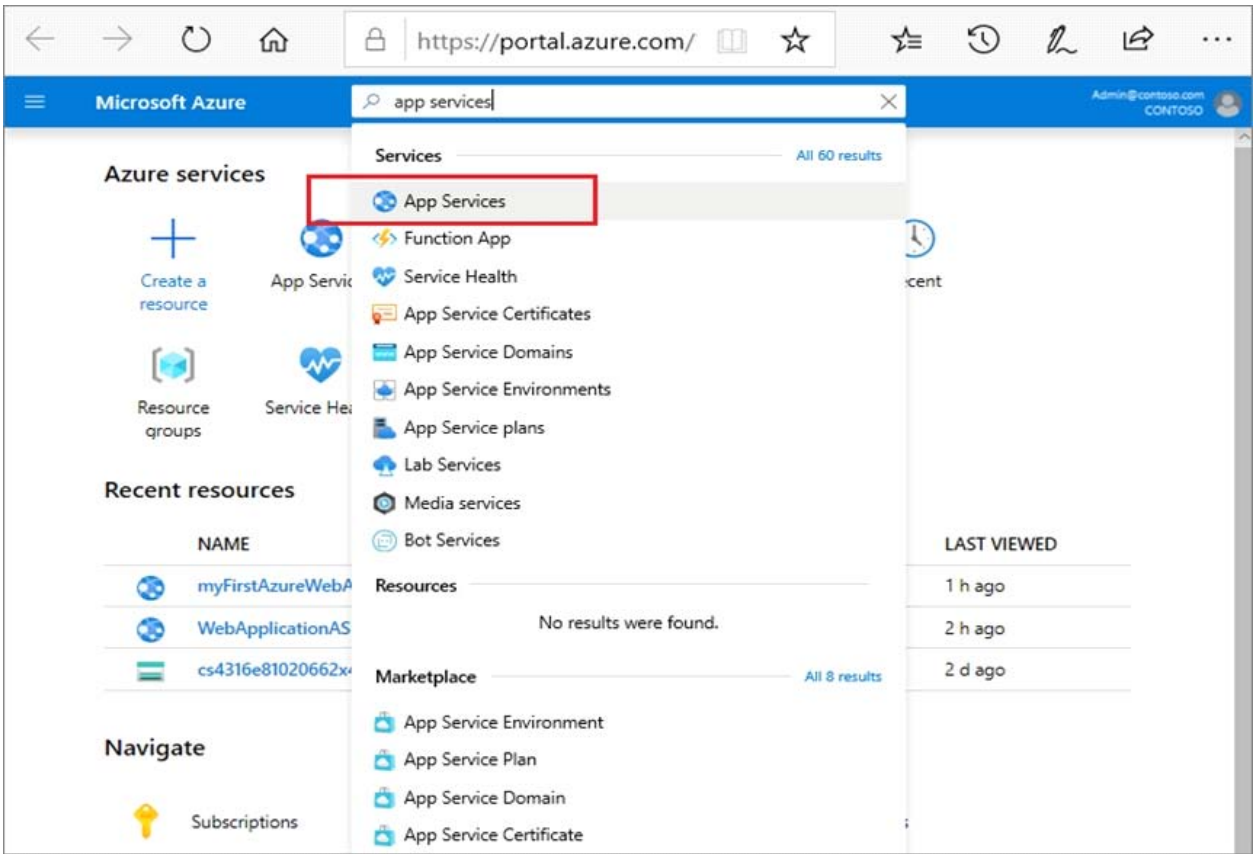
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

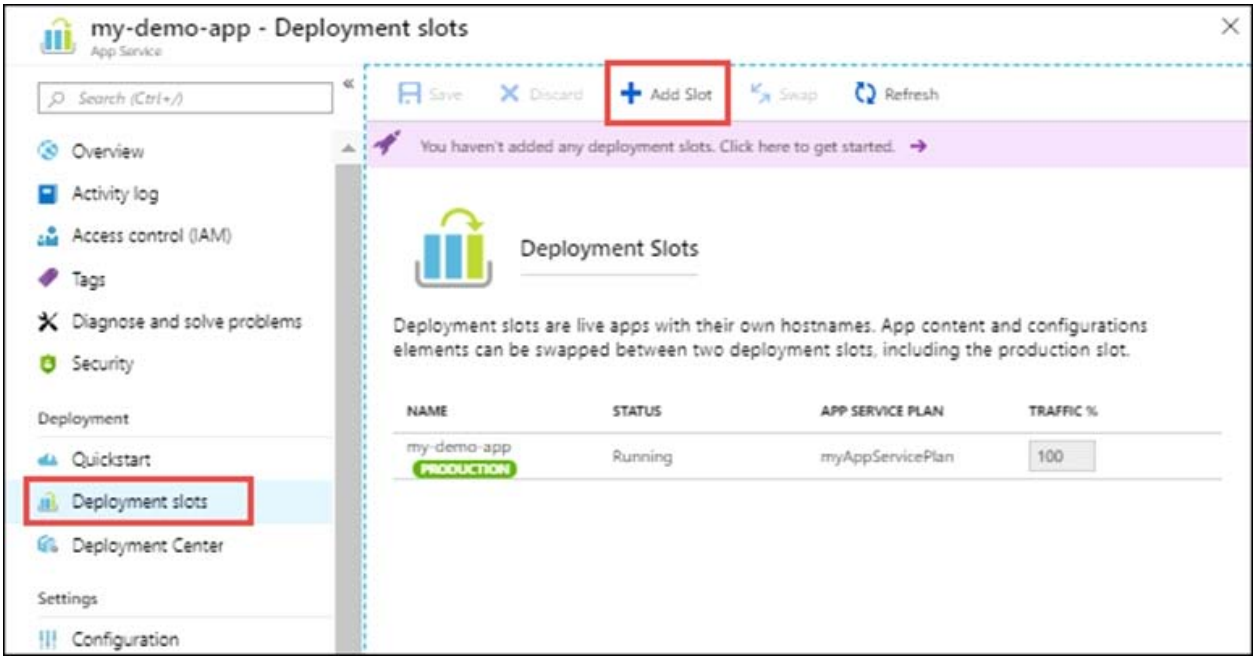
Explanation:

Add a slot

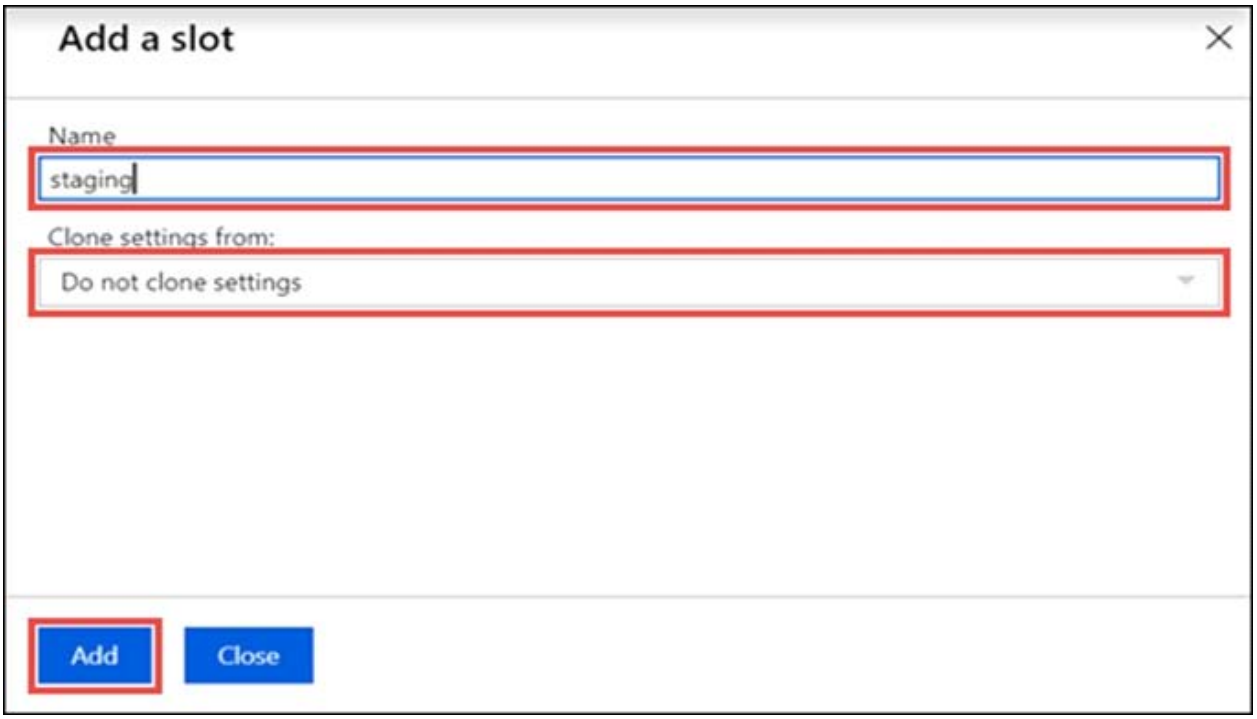
1. In the Azure portal, search for and select App Services and select your app az400-11566895-main.



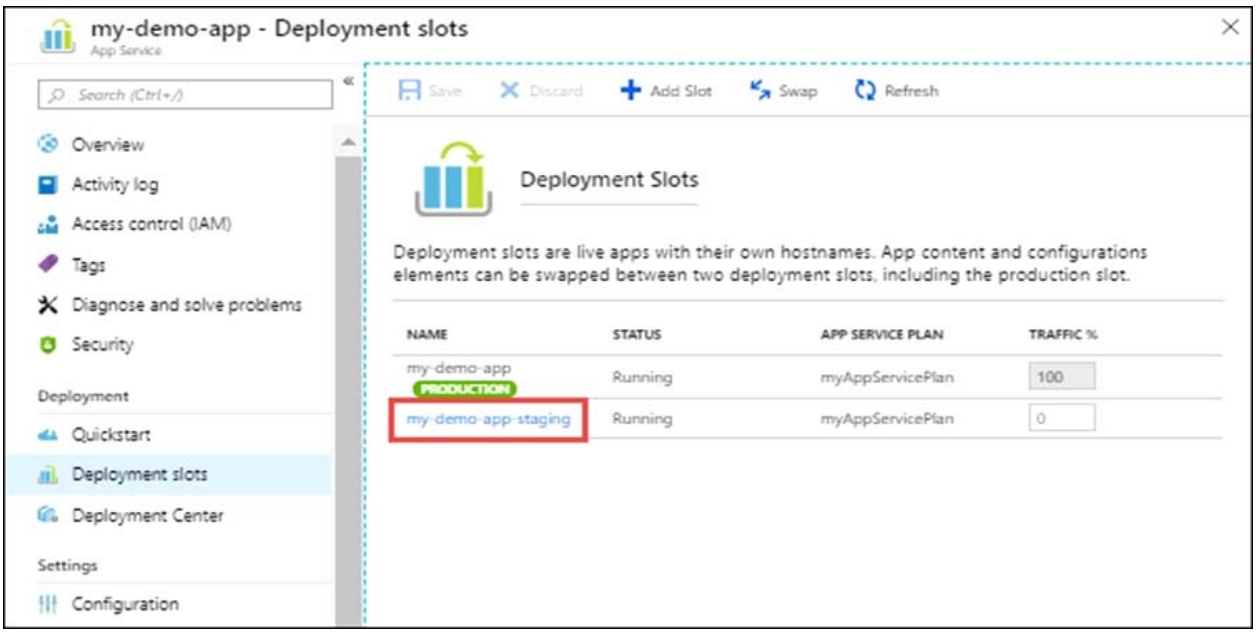
2. In the left pane, select Deployment slots > Add Slot.



3. In the Add a slot dialog box, give the slot a name, and select whether to clone an app configuration from another deployment slot. Select Add to continue.



4. After the slot is added, select Close to close the dialog box. The new slot is now shown on the Deployment slots page.



Reference:
https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots

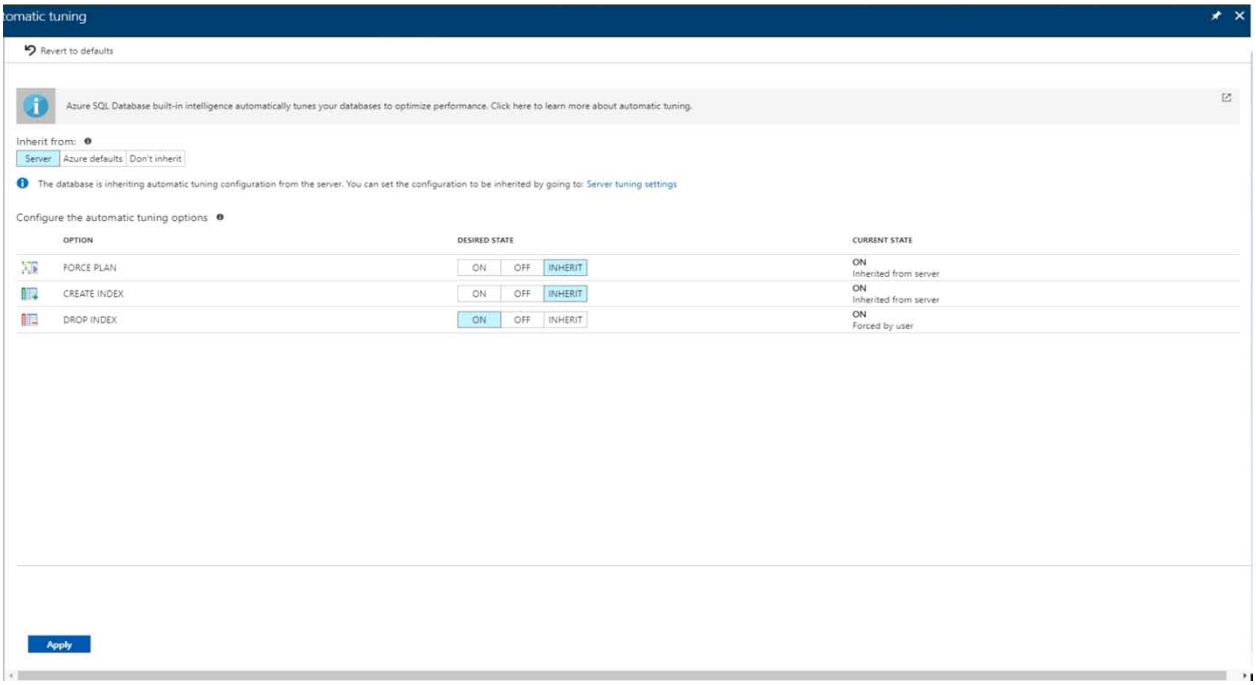
Question: 185

You have several apps that use an Azure SQL Database named db1.

You need to ensure that queries to db1 are tuned by Azure over time. The solution must only apply to db1.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
1. To enable automatic tuning on a single database, navigate to the database in the Azure portal and select Automatic tuning.



2. Select the automatic tuning options you want to enable and select Apply.
Note: Individual automatic tuning settings can be separately configured for each database. You can manually configure an individual automatic tuning option, or specify that an option inherits its settings from the server.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/automatic-tuning-enable

Question: 186

You administer an Azure DevOps project that includes package feeds.
You need to ensure that developers can unlist and deprecate packages. The solution must use the principle of least privilege.
Which access level should you grant to the developers?

A. Collaborator
B. Contributor
C. Owner

Answer: B

Explanation:
Feeds have four levels of access: Owners, Contributors, Collaborators, and Readers. Owners can add any type of identity-individuals, teams, and groups-to any access level.

Permission	Reader	Collaborator	Contributor	Owner
List and restore/install packages	✓	✓	✓	✓
Save packages from upstream sources		✓	✓	✓
Push packages			✓	✓
Unlist/deprecate packages			✓	✓
Promote a package to a view			✓	✓
Delete/unpublish package				✓
Edit feed permissions				✓

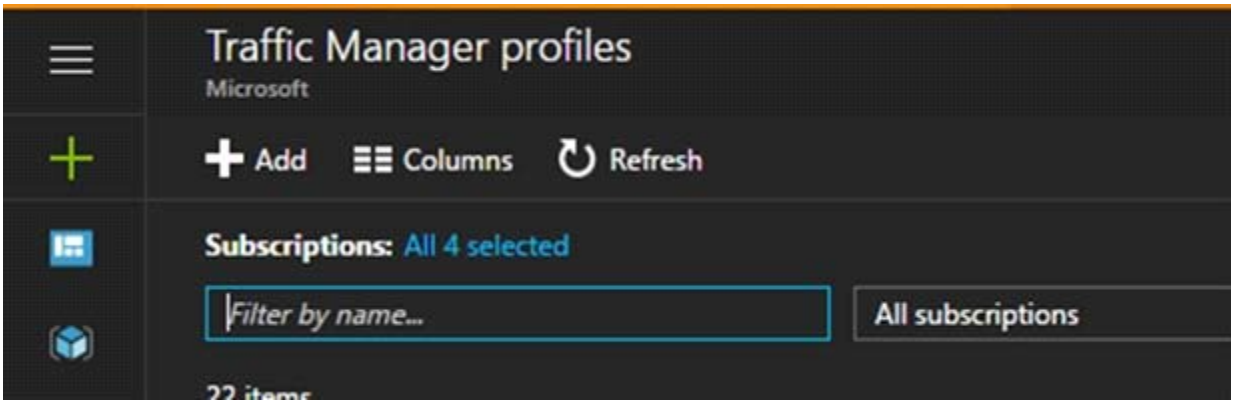
Reference:
https://docs.microsoft.com/en-us/azure/devops/artifacts/feeds/feed-permissions

Question: 187

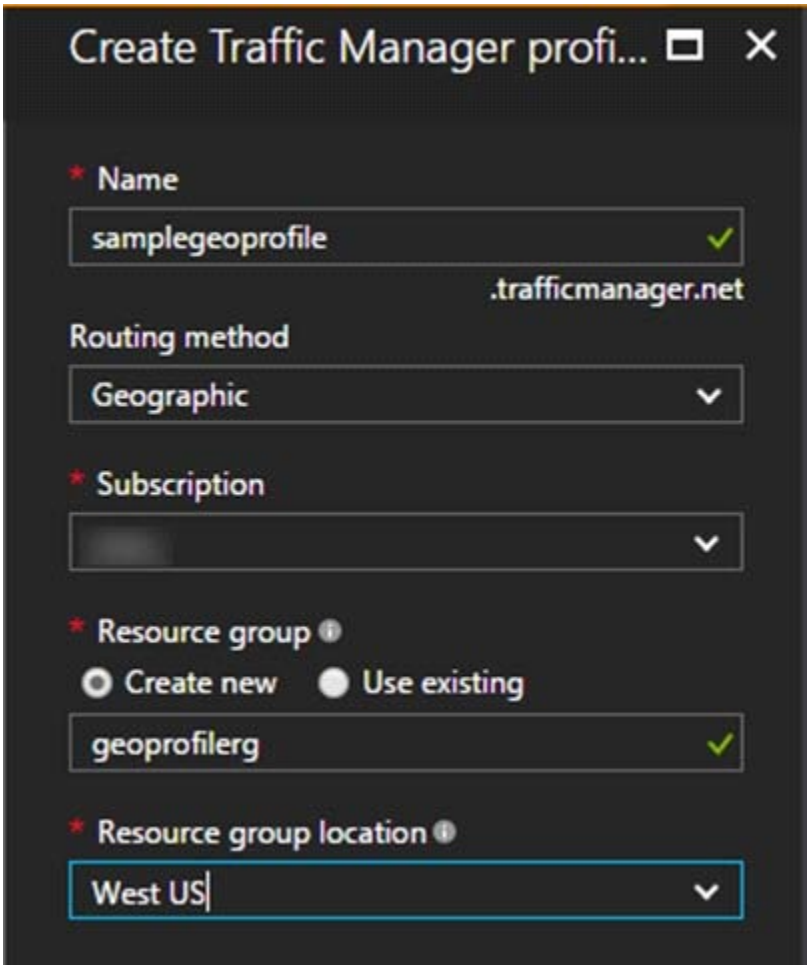
You plan to deploy a website that will be hosted in two Azure regions.
You need to create an Azure Traffic Manager profile named az40011566895n1-tm in a resource group named RG1lod11566895. The solution must ensure that users will always connect to a copy of the website that is in the same country.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
1. Go to the Azure portal, navigate to Traffic Manager profiles and click on the Add button to create a routing profile.



2. In the Create Traffic Manager profile, enter, or select these settings:
Name: az40011566895n1-tm
Routing method: Geographic
Resource group: RG1lod11566895



Note: Traffic Manager profiles can be configured to use the Geographic routing method so that users are directed to specific endpoints (Azure, External or Nested) based on which geographic location their DNS query originates from. This empowers Traffic Manager customers to enable scenarios where knowing a user's geographic region and routing them based on that is important.

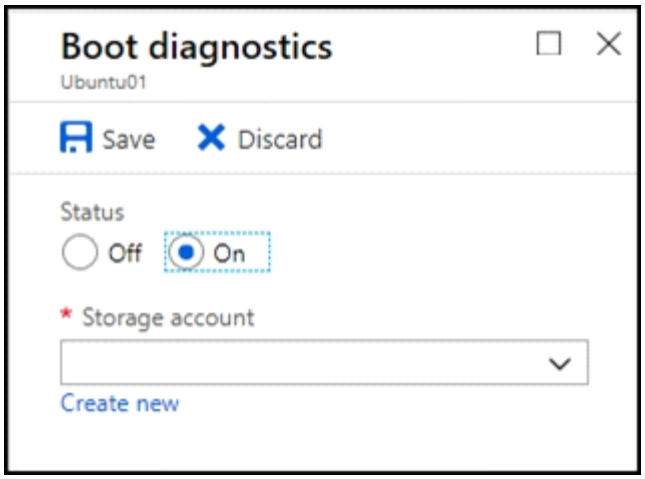
Reference:
https://azure.microsoft.com/en-us/blog/announcing-the-general-availability-of-geographic-routing-capability-in-azure-traffic-manager/

Question: 188

You need to create and configure an Azure Storage account named az400lod11566895stor in a resource group named RG1lod11566895 to store the boot diagnostics for a virtual machine named VM1.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

Explanation:
Step 1: To create a general-purpose v2 storage account in the Azure portal, follow these steps:
On the Azure portal menu, select All services. In the list of resources, type Storage Accounts. As you begin typing, the list filters based on your input. Select Storage Accounts.
On the Storage Accounts window that appears, choose Add.
Select the subscription in which to create the storage account.
Under the Resource group field, select RG1lod11566895
Next, enter a name for your storage account named: az400lod11566895stor
Select Create.
Step 2: Enable boot diagnostics on existing virtual machine
To enable Boot diagnostics on an existing virtual machine, follow these steps:
1. Sign in to the Azure portal, and then select the virtual machine VM1.
2. In the Support + troubleshooting section, select Boot diagnostics, then select the Settings tab.
3. In Boot diagnostics settings, change the status to On, and from the Storage account drop-down list, select the storage account az400lod11566895stor.
4. Save the change.



You must restart the virtual machine for the change to take effect.
Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-account-create
https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/boot-diagnostics

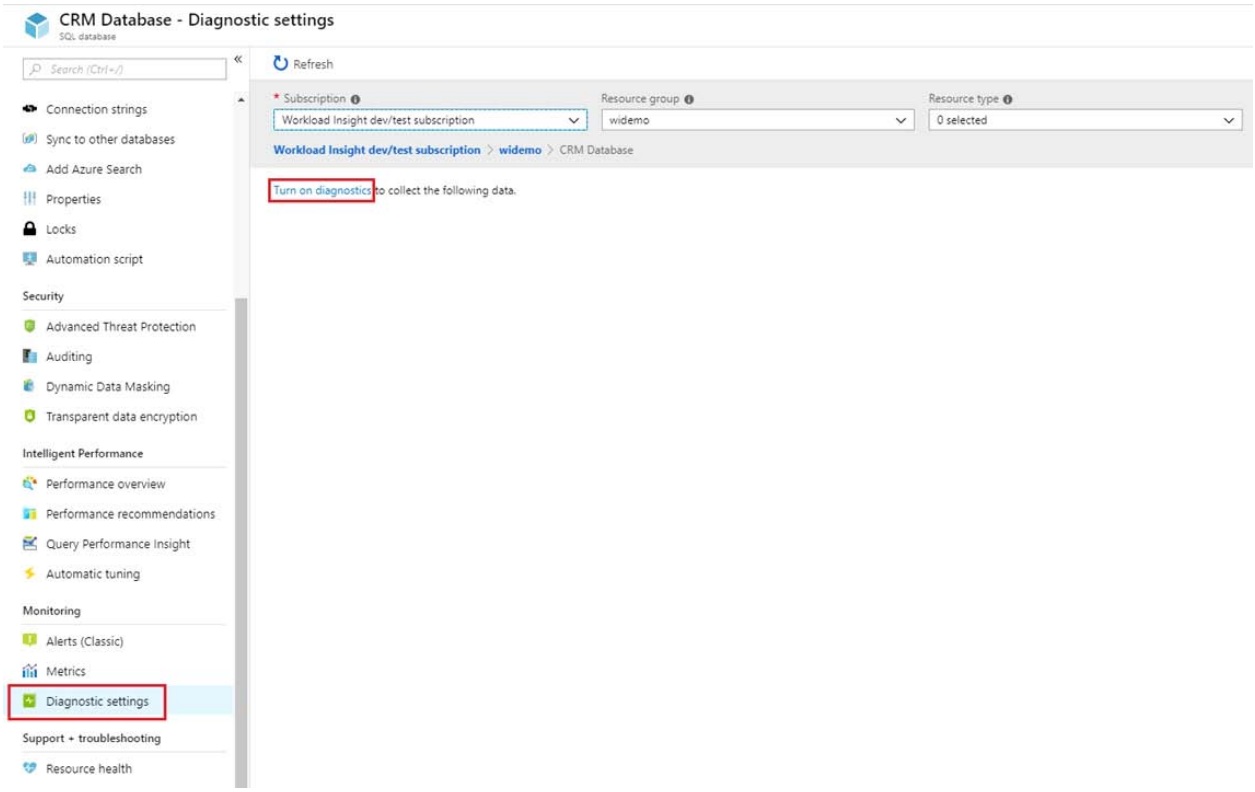
Question: 189

You have a web app that connects to an Azure SQL Database named db1.
You need to configure db1 to send Query Store runtime statistics to Azure Log Analytics.
To complete this task, sign in to the Microsoft Azure portal.

Answer: See solution below.

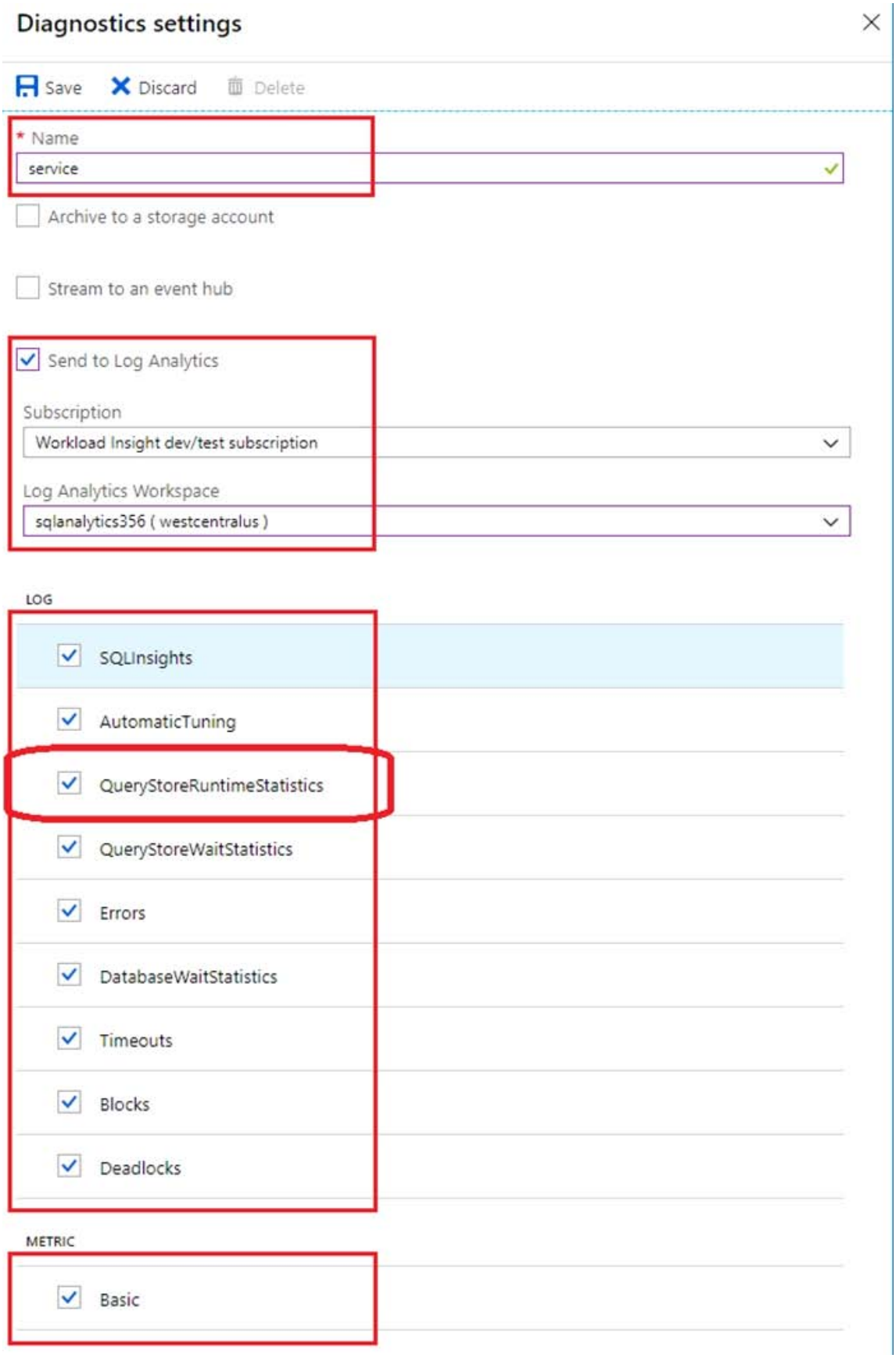
Explanation:

To enable streaming of diagnostic telemetry for a single or a pooled database, follow these steps:
1. Go to Azure SQL database resource.
2. Select Diagnostics settings.
3. Select Turn on diagnostics if no previous settings exist, or select Edit setting to edit a previous setting. You can create up to three parallel connections to stream diagnostic telemetry.
4. Select Add diagnostic setting to configure parallel streaming of diagnostics data to multiple resources.



5. Enter a setting name for your own reference.

6. Select a destination resource for the streaming diagnostics data: Archive to storage account, Stream to an event hub, or Send to Log Analytics.
7. For the standard, event-based monitoring experience, select the following check boxes for database diagnostics log telemetry: QueryStoreRuntimeStatistics


Diagnostics settings
Save
Discard
Delete
* Name
service
Archive to a storage account
Stream to an event hub
Send to Log Analytics
Subscription
Workload Insight dev/test subscription
Log Analytics Workspace
sqlanalytics356 (westcentralus)
LOG
SQLInsights
AutomaticTuning
QueryStoreRuntimeStatistics
QueryStoreWaitStatistics
Errors
DatabaseWaitStatistics
Timeouts
Blocks
Deadlocks
METRIC
Basic

8. For an advanced, one-minute-based monitoring experience, select the check box for Basic metrics.
9. Select Save.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure

Question: 199

Your company is building a new solution in Java.
The company currently uses a SonarQube server to analyze the code of .NET solutions.
You need to analyze and monitor the code quality of the Java solution.
Which task types should you add to the build pipeline?

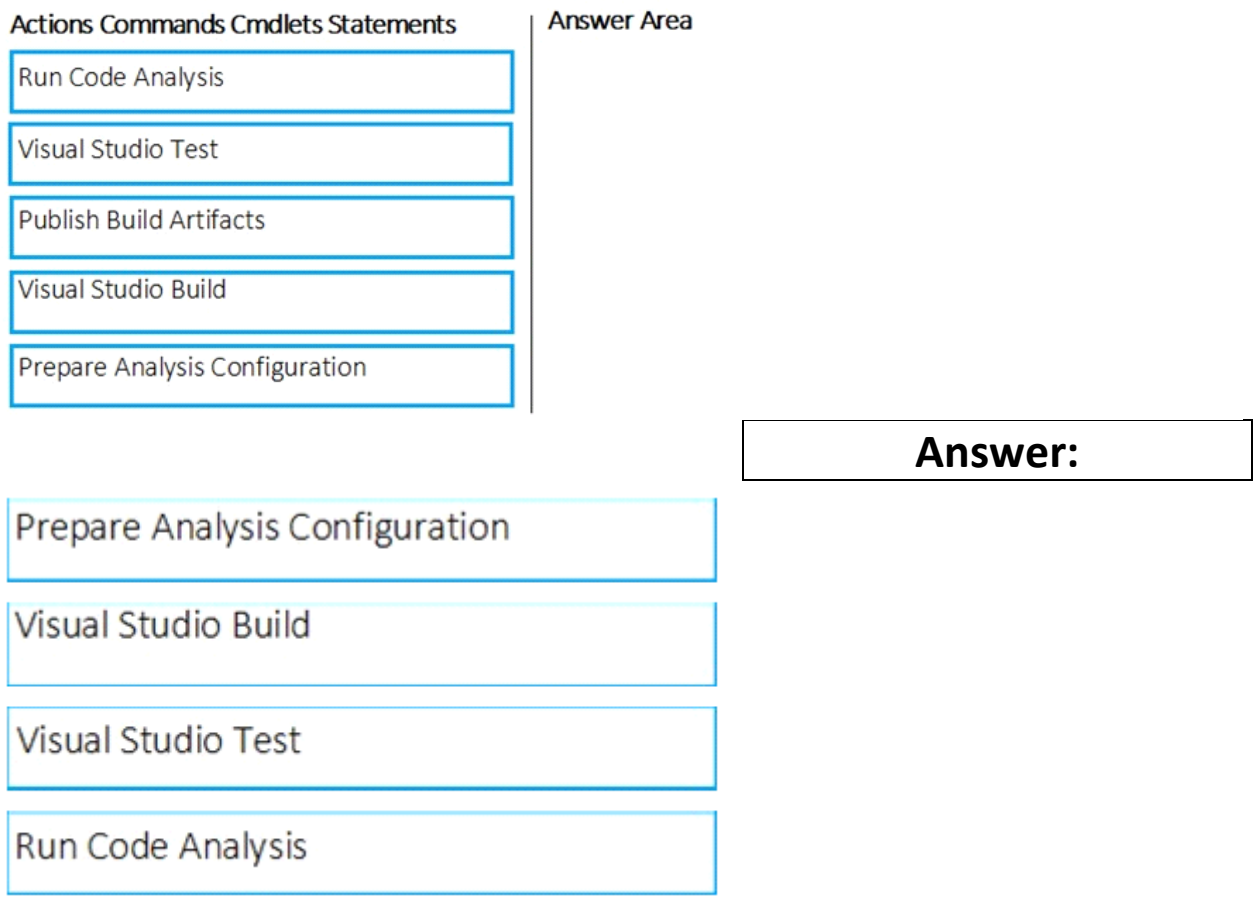
A. Chef
B. Gradle
C. Octopus
D. Gulp

Answer: B

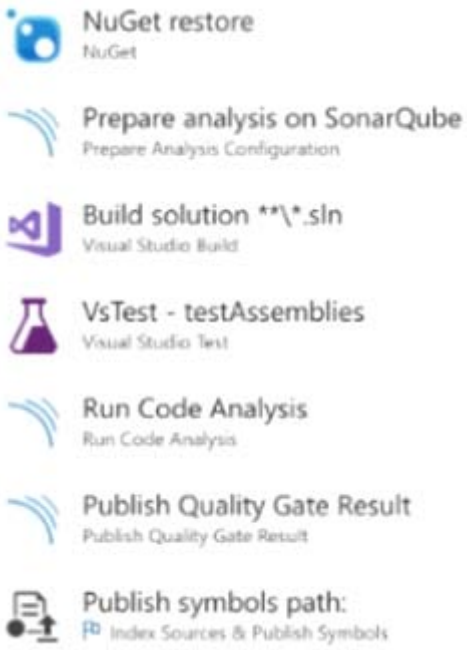
Explanation:
SonarQube is a set of static analyzers that can be used to identify areas of improvement in your code. It allows you to analyze the technical debt in your project and keep track of it in the future. With Maven and Gradle build tasks, you can run SonarQube analysis with minimal setup in a new or existing Azure DevOps Services build task.
References:
https://docs.microsoft.com/en-us/azure/devops/java/sonarqube?view=azure-devops

Question: 200

You are developing a full Microsoft .NET Framework solution that includes unit tests.
You need to configure SonarQube to perform a code quality validation of the C# code as part of the build pipelines.
Which four tasks should you perform in sequence? To answer, move the appropriate tasks from the list of tasks to the answer area and arrange them in the correct order.



Explanation:
Step 1: Prepare Analysis Configuration
Prepare Analysis Configuration task, to configure all the required settings before executing the build.
This task is mandatory.
In case of .NET solutions or Java projects, it helps to integrate seamlessly with MSBuild, Maven and Gradle tasks.
Step 2: Visual Studio Build
Reorder the tasks to respect the following order:
Prepare Analysis Configuration task before any MSBuild or Visual Studio Build task.
Step 3: Visual Studio Test
Reorder the tasks to respect the following order:
Run Code Analysis task after the Visual Studio Test task.
Step 4: Run Code Analysis
Run Code Analysis task, to actually execute the analysis of the source code.
This task is not required for Maven or Gradle projects, because scanner will be run as part of the Maven/Gradle build.
Note:



References:
https://docs.sonarqube.org/display/SCAN/Analyzing+with+SonarQube+Extension+for+VSTS-TFS

Thank You for Trying Our Product

Discount Coupon Code:
EXAMSBOOST10

For More Information – **Visit link below:**

http://www.examsboost.com/

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer