



Vendor: Microsoft

Exam Code: AZ-400

Exam Name: Microsoft Azure DevOps Solutions

Version: 21.021

Important Notice

Product

Our Product Manager keeps an eye for Exam updates by Vendors. Free update is available within One year after your purchase.

You can login member center and download the latest product anytime. (Product downloaded from member center is always the latest.)

PS: Ensure you can pass the exam, please check the latest product in 2-3 days before the exam again.

Feedback

We devote to promote the product quality and the grade of service to ensure customers interest.

If you have any questions about our product, please provide Exam Number, Version, Page Number, Question Number, and your Login Account to us, please contact us at support@passleader.com and our technical experts will provide support in 24 hours.

Copyright

The product of each order has its own encryption code, so you should use it independently.

If anyone who share the file we will disable the free update and account access.

Any unauthorized changes will be inflicted legal punishment. We will reserve the right of final explanation for this statement.

Order ID: ****

PayPal Name: ****

PayPal ID: ****

Case Study 1 - Litware (QUESTION 1 - QUESTION 5)

Overview

Existing Environment

Litware, Inc. is 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.NET web forms that use logic written in VB.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 live 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 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.

Customers report that bug reporting is overly complex.

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 existing retirement fund management system.

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.

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

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

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

Technical requirements

The company's investment planning applications suite must meet the following 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 releases must remain available for 30 days, except for production releases, which must be kept for 60 days.
- 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 HTTPS.
- The required operating system configuration for the test servers changes weekly. Azure Automation State Configuration must be used to ensure that the operating system on each test server is configured the same way when the servers are created and checked periodically.

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'
```

QUESTION 1

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 2

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: 

Explanation: 

When a release is created from a release pipeline that defines approvals, the deployment stops at each point where approval is required until the specified approver grants approval or rejects the release (or re-assigns the approval to another user).

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

References:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/approvals>

QUESTION 3

Hotspot Question

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 Area

```
MSAppCenter.start  
( "{Your App Secret}",  
  withServices:  
)
```

[MSAnalytics.self,
[MSDistribute.self,
[MSPush.self,

MSAnalytics.self]
MSCrashes.self]
MSDistribute.self]

Answer:

Answer Area

```
MSAppCenter.start  
( "{Your App Secret}",  
  withServices:  
)
```



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 4

Hotspot Question

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 Area

Global release:

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

Production stage:

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

Answer:

Answer Area

Global release:

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

Production stage:

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

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 5

Hotspot Question

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 in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Required secrets:

Certificate
Personal access token
Shared Access Authorization token
Username and password

Storage location:

Azure Data Lake
Azure Key Vault
Azure Storage with HTTP access
Azure Storage with HTTPS access

Answer:



Answer Area

Required secrets:

Certificate
Personal access token
Shared Access Authorization token
Username and password

Storage location:

Azure Data Lake
Azure Key Vault
Azure Storage with HTTP access
Azure Storage with HTTPS access

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>

Case Study 2 - Contoso, Ltd (QUESTION 6 - QUESTION 11)

Background

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

Contoso plans to improve its IT development and operations processes by implementing Azure 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.

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 identifies the following technical requirements:

- Implement build agents for Project1.
- Whenever possible, use Azure resources.
- Avoid using deprecated technologies.
- 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.
 - Whenever possible implement automation and minimize administrative effort.
- Implement Project3, Project5, Project6, and Project7 based on the planned changes
- Implement Project4 and configure the project to push Docker images to Azure Container Registry.

QUESTION 6

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

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 7

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: 

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 8

Drag and Drop Question

You need to configure Azure Automation for the computers 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.

Actions	Answer Area
Run the <code>Import-AzureRmAutomationDscConfiguration</code> Azure PowerShell cmdlet.	
Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1.	
Run the <code>New-AzureRmResourceGroupDeployment</code> Azure PowerShell cmdlet.	⟳ ⟳
Run the <code>Start-AzureRmAutomationDscCompilationJob</code> Azure PowerShell cmdlet.	
Create an Azure Resource Manager template file that has an extension of .json.	

Answer:

Actions	Answer Area
	Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1.
	Run the <code>Import-AzureRmAutomationDscConfiguration</code> Azure PowerShell cmdlet.
Run the <code>New-AzureRmResourceGroupDeployment</code> Azure PowerShell cmdlet.	⟳ ⟳
	Run the <code>Start-AzureRmAutomationDscCompilationJob</code> Azure PowerShell cmdlet.
Create an Azure Resource Manager template file that has an extension of .json.	

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 9

Hotspot Question

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 Area

Set a

branch filter to exclude
branch filter to include
path filter to exclude
path filter to include

/folder1.

Set a

branch filter to exclude
branch filter to include
path filter to exclude
path filter to include

/.

@

Answer:**Answer Area**

Set a

branch filter to exclude
branch filter to include
path filter to exclude
path filter to include

/folder1.

Set a

branch filter to exclude
branch filter to include
path filter to exclude
path filter to include

/.

@

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 10**

Drag and Drop Question

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

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange in the correct order.

Actions	Answer Area
Create a fork	
Create a branch	
Add a build validation policy.	
Add a build policy	
Create a repository	
Add an application access policy.	

Answer:

Actions

Create a fork

Add a build validation policy.

Answer Area

Create a repository

Create a branch

Add a build policy

**Add an application access 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 11

Drag and Drop Question

You need to implement Project6.

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

Actions
Answer Area

Open the release pipeline editor.

Disable the continuous integration trigger.

Enable Gates.



Add a manual intervention task.

 Open the **Triggers** tab.

Add Query Work Items.

Answer:
Actions
Answer Area

Open the release pipeline editor.

Disable the continuous integration trigger.



Enable Gates.

Add a manual intervention task.

 Open the **Triggers** tab.

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.

Deployment gates ⓘ

+ Add ▾

Query Work Items Enabled ⚡

Query Work Items ⓘ

Task version 0.* ▾

Display name *

Query Work Items

Query * ⓘ

Active Bugs ▾

Upper threshold * ⓘ

0

Advanced ^

Lower threshold * ⓘ

0

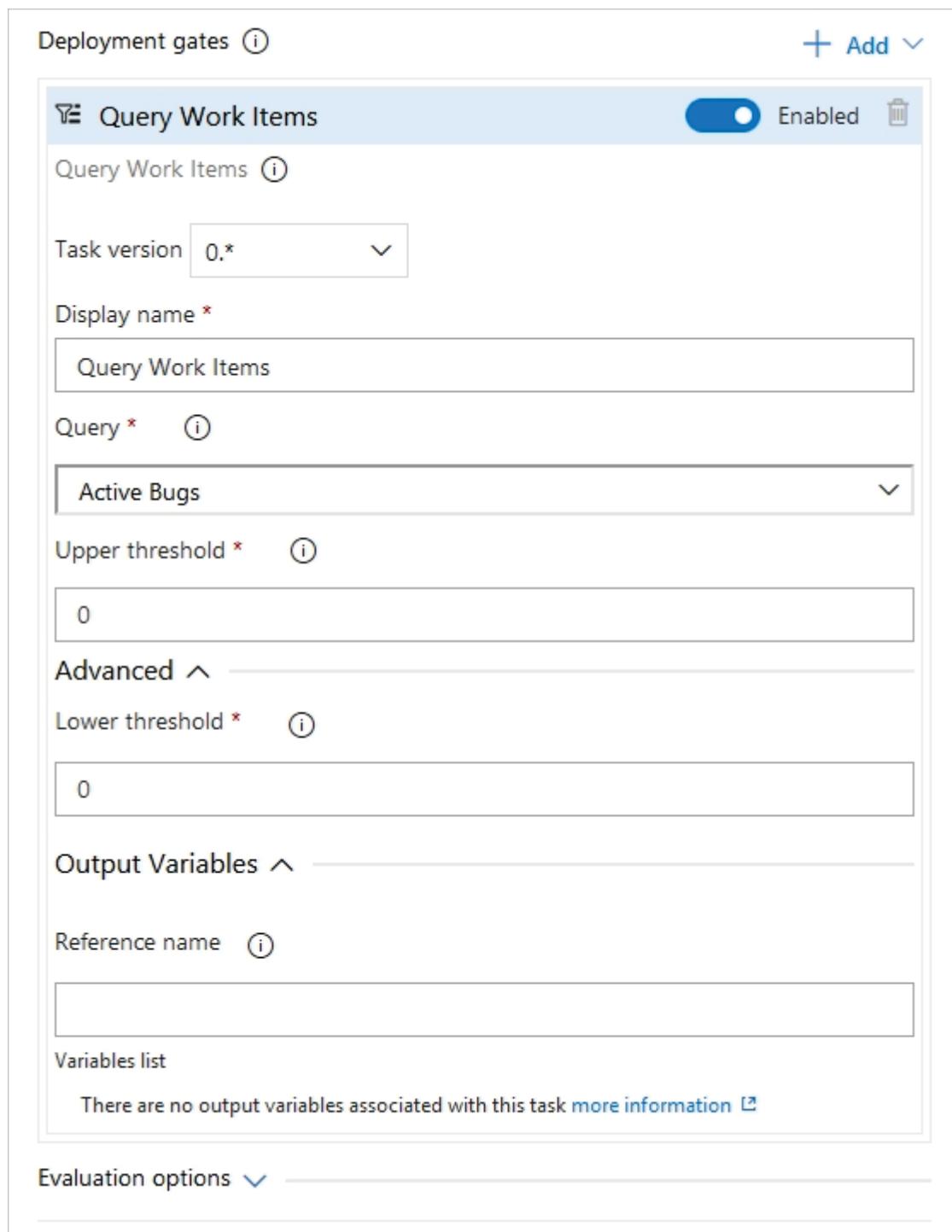
Output Variables ^

Reference name ⓘ

Variables list

There are no output variables associated with this task [more information ↗](#)

Evaluation options ▾



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 12

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You integrate a cloud-hosted Jenkins server and a new Azure DevOps deployment

You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.

Solution: You create a service hook subscription that uses the code pushed event.

Does this meet the goal?

- A. Yes
- B. NO

Answer: A

Explanation:

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

References:

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

QUESTION 13

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 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 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 14

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 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 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 15

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 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 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 16

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 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 Timeout setting for pre-deployment approvals.

Does this meet the goal?

- A. Yes
- B. No

Answer: 

Explanation:

Use a gate instead of an approval instead.

References:

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

QUESTION 17

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: 

Explanation:

In Visual Designer you enable continuous integration (CI) by:

1. Select the Triggers tab.
2. Enable Continuous integration.

A continuous integration trigger on a build pipeline indicates that the system should automatically queue a new build whenever a code change is committed.

References:

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

QUESTION 18

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 selected Batch changes while a build is in progress

Does this meet the goal?

- A. Yes
- B. No

Answer: B

QUESTION 19

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 it meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

In Visual Studio you enable continuous integration (CI) by:

1. Select the Triggers tab.
2. Enable Continuous integration.

References:

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

QUESTION 20

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: A

Explanation:

Multi-stage builds (in Docker 17.05 or higher) allow you to drastically reduce the size of your final image, without struggling to reduce the number of intermediate layers and files. With multi-stage builds, you use multiple FROM statements in your Dockerfile. Each FROM instruction can use a different base, and each of them begins a new stage of the build. You can selectively copy artifacts from one stage to another, leaving behind everything you don't want in the final image.

References:

<https://docs.docker.com/develop/develop-images/multistage-build/#use-multi-stage-builds>

QUESTION 21

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 22

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.

References:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-code-coverage-results>

QUESTION 23

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

- Minimizes image sizes
- Minimizes the security surface area of the final image

What should you include in the recommendation?

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

D. Docker Swarm

Answer: A

Explanation:

Multi-stage builds are a new feature requiring Docker 17.05 or higher on the daemon and client. Multistage builds are useful to anyone who has struggled to optimize Dockerfiles while keeping them easy to read and maintain.

References:

<https://docs.docker.com/develop/develop-images/multistage-build/>

QUESTION 24

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 will 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 in 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 25

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

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

You need to automate the management of users and licenses whenever possible.

Which task must you perform manually?

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

Answer: B

Explanation:

<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 26

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 27

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 28

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: A



QUESTION 29

Your company deploys applications in Docker containers.

You want to detect known exploits in the Docker 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 30

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: 

Explanation:

Application Map helps you spot performance bottlenecks or failure hotspots across all components of your distributed application. Each node on the map represents an application component or its dependencies; and has health KPI and alerts status.

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-map>

QUESTION 31

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.

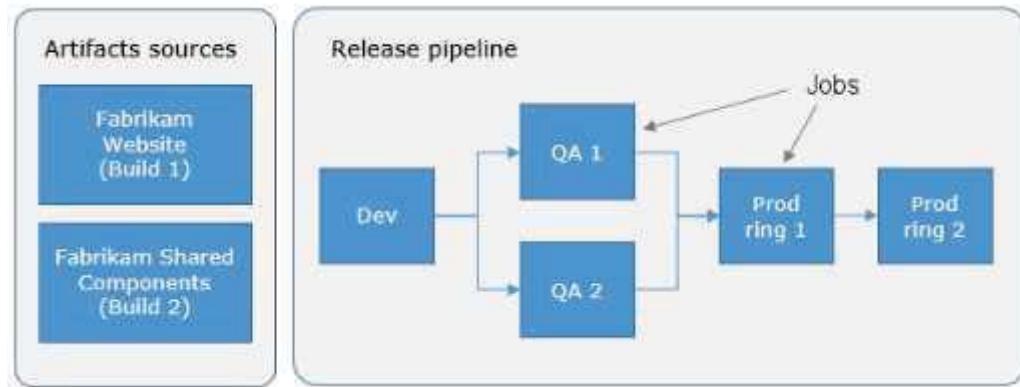
NOTE: Each correct selection is worth one point.

- 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: 

Explanation:

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



In this example, a release of a website is created by collecting specific versions of two builds (artifacts), each from a different build pipeline. The release is first deployed to a Dev stage and then forked to two QA stages in parallel. If the deployment succeeds in both the QA stages, the release is deployed to Prod ring 1 and then to Prod ring 2. Each production ring represents multiple instances of the same website deployed at various locations around the globe.

References:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/release>

QUESTION 32

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 point.

- 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

Explanation:

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 33

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

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

What should you do?

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

Answer: B

Explanation:

In some cases, you need to bypass policy requirements so you can push changes to the branch directly or complete a pull request even if branch policies are not satisfied. For these situations, grant the desired permission from the previous list to a user or group. You can scope this permission to an entire project, a repo, or a single branch. Manage this permission along with other Git permissions.

References:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies>

QUESTION 34

You have an Azure Resource Manager template that deploys a multi-tier application.

You need to prevent the user who performs the deployment from viewing the account credentials and connection strings used by the application.

What should you use?

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

Answer: D

Explanation:

When you need to pass a secure value (like a password) as a parameter during deployment, you can retrieve the value from an Azure Key Vault. You retrieve the value by referencing the key vault and secret in your parameter file. The value is never exposed because you only reference its key vault ID. The key vault can exist in a different subscription than the resource group you are deploying to.

References:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter>

QUESTION 35

Your company uses a Git repository in Azure Repos to manage the source code of a web

application. The master branch is protected from direct updates. Developers work on new features in the topic branches.

Because of the high volume of requested features, it is difficult to follow the history of the changes to the master branch.

You need to enforce a pull request merge strategy. The strategy must meet the following requirements:

- Consolidate commit histories
- Merge tie changes into a single commit

Which merge strategy should you use in the branch policy?

- A. Git fetch
- B. no-fast-forward merge
- C. squash merge
- D. fast-forward merge

Answer: C

Explanation:

Squash merging is a merge option that allows you to condense the Git history of topic branches when you complete a pull request. Instead of each commit on the topic branch being added to the history of the default branch, a squash merge takes all the file changes and adds them to a single new commit on the default branch.

A simple way to think about this is that squash merge gives you just the file changes, and a regular merge gives you the file changes and the commit history.

Note: Squash merging keeps your default branch histories clean and easy to follow without demanding any workflow changes on your team. Contributors to the topic branch work how they want in the topic branch, and the default branches keep a linear history through the use of squash merges. The commit history of a master branch updated with squash merges will have one commit for each merged branch. You can step through this history commit by commit to find out exactly when work was done.

References:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/merging-with-squash>

QUESTION 36

Your company uses cloud-hosted Jenkins for builds.

You need to ensure that Jenkins can retrieve source code from Azure Repos.

Which three actions should you perform? Each correct answer presents part of the solution

NOTE: Each correct answer selection is worth one point

- A. Add the Team Foundation Server (TFS) plug-in to Jenkins.
- B. Create a personal access token in your Azure DevOps account.
- C. Create a webhook in Jenkins.
- D. Add a domain to your Jenkins account.
- E. Create a service hook in Azure DevOps.

Answer: ABE

Explanation:

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

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

QUESTION 37

You are developing an open source solution that uses a GitHub repository.

You create a new public project in Azure DevOps.

You plan to use Azure Pipelines for continuous build. The solution will use the GitHub Checks API.

Which authentication type should you use?

- A. a personal access token
- B. SAML
- C. GitHub App
- D. OAuth

Answer: 

Explanation: 

You can authenticate as a GitHub App.

References:

<https://developer.github.com/apps/building-github-apps/authenticating-with-github-apps/>

QUESTION 38

You plan to share packages that you wrote, tested, validated, and deployed by using Azure Artifacts.

You need to release multiple builds of each package by using a single feed. The solution must limit the release of packages that are in development.

What should you use?

- A. global symbols
- B. local symbols
- C. upstream sources
- D. views

Answer: 

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 39

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 40

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

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

What should you use?

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

Answer: C

Explanation:

Secure and Manage Open Source Software

Black Duck helps organizations identify and mitigate open source security, license compliance and code-quality risks across application and container portfolios.

Black Duck Hub and its plugin for Team Foundation Server (TFS) allows you to automatically find and fix open source security vulnerabilities during the build process, so you can proactively manage risk. The integration allows you to receive alerts and fail builds when any Black Duck Hub policy violations are met.

Note: WhiteSource would also be a good answer, but it is not an option here.

References:

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

QUESTION 41

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 42

You use Azure SQL Database Intelligent Insights and Azure Application Insights for monitoring. You need to write ad-hoc Queries against the monitoring data.

Which Query language should you use?

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

Answer: C

Explanation:

Data analysis in Azure SQL Analytics is based on Log Analytics language for your custom querying and reporting.

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-sql>

QUESTION 43

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 ImiQ.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 44

You have multi-tier application that has an Azure Web Apps front end and an Azure SQL Database back end.

You need to recommend a solution to capture and store telemetry data. The solution must meet the following requirements:

- Support using ad-hoc queries to identify baselines.
- Trigger alerts when metrics in the baseline are exceeded.
- Store application and database metrics in a central location.

What should you include in the recommendation?

- A. Azure Application 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 45

Your company creates a web application.

You need to recommend a solution that automatically sends to Microsoft Teams a daily summary of the exceptions that occur in 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

Explanation:

<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 46

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 47

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:

Use a Pull request trigger.

References:

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

QUESTION 48

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 49

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: 

Explanation:

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

References:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates> Approvals and gates give you additional control over the start and completion of the deployment pipeline. Each stage in a release pipeline can be configured with pre-deployment and post-deployment conditions that can include waiting for users to manually approve or reject deployments, and checking with other automated systems until specific conditions are verified.

QUESTION 50

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: 
Explanation:

Use a main template and two linked templates.

References:

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

QUESTION 51

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 52

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 53

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:

1. Detect and remedy vulnerable open source components.
2. Generate comprehensive open source inventory reports per project or build.
3. Enforce open source license compliance, including dependencies' licenses.
4. Identify outdated open source libraries with recommendations to update.

References:

<https://www.azuredevopslabs.com/labs/vstsextend/WhiteSource/>

QUESTION 54

Drag and Drop Question

You have an Azure Kubernetes 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.

Actions**Answer Area**

Run helm init.



Create a YAML file.



Run az aks install-connector.

Run az role assignment create

Run kubectl apply.

Answer:

Actions

Run az aks install-connector.

Run az role assignment create

Answer Area

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 55

Drag and Drop Question

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 is correct. You will receive credit for any of the orders you select.

Actions

Onboard the virtual machines to Azure Automation State Configuration.

Check the compliance status of the node.

Create a management group.

Assign the node configuration.

Answer Area

Compile a configuration into a node configuration.

Upload a configuration to Azure Automation State Configuration.

Assign tags to the virtual machines.

Answer:**Actions**

Create a management group.

Answer Area

Assign the node configuration.

Upload a configuration to Azure Automation State Configuration.

Compile a configuration into a node configuration.



Onboard the virtual machines to Azure Automation State Configuration.

Assign tags to the virtual machines.

Check the compliance status of the node.

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 56

Hotspot Question

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 secrets stored in Azure Key Vault.

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

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

NOTE: Each correct selection is worth one point.

```

"resources": [
{
    "apiversion": "2018-05-01",
    "name" : "secrets",
    "type": "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 57

Drag and Drop Question

Your company has a project in Azure DevOps.

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

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

What should you include in the recommendation? To answer, drag the appropriate configurations to the correct targets. Each configuration may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Configurations
Answer Area

A Key Vault access policy

Enable key vaults for template deployment by using:

A Key Vault advanced access policy

Restrict access to the secrets in Key Vault by using:

RBAC

Answer:

Configurations
Answer Area

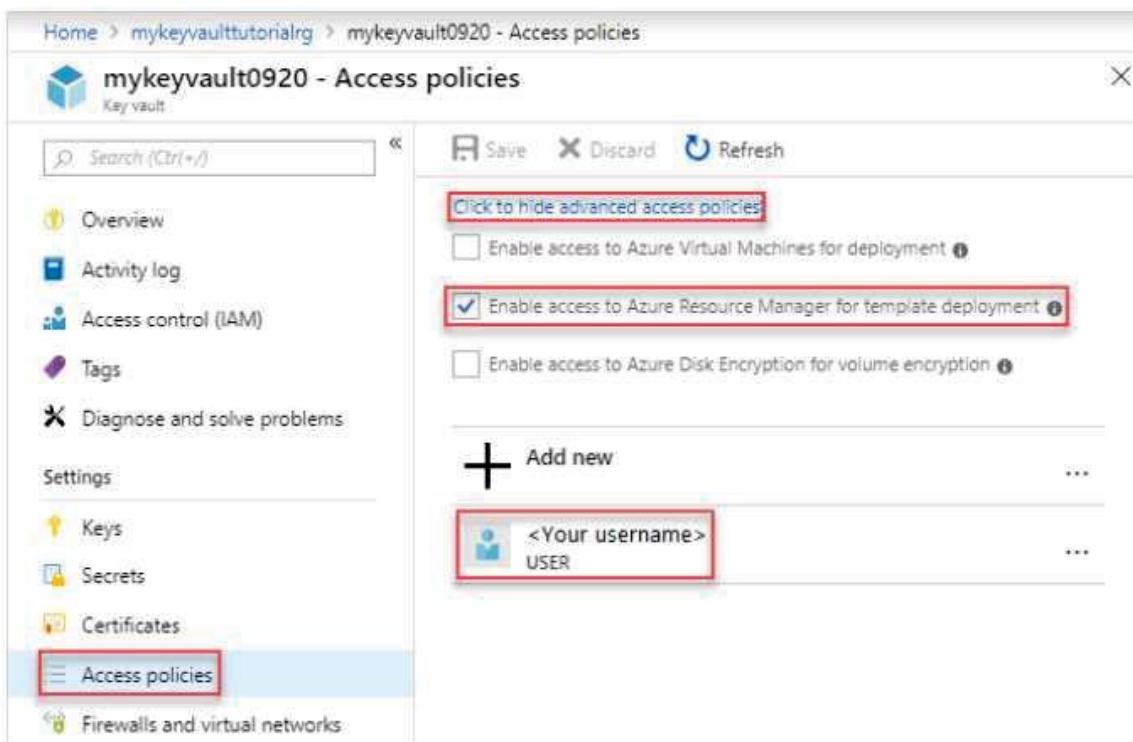
A Key Vault access policy

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



The screenshot shows the Azure portal interface for managing access policies in a Key Vault. The left sidebar lists various management options like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The 'Access policies' option is selected and highlighted with a red box. The main content area shows a list of checkboxes for enabling different types of access. The checkbox for 'Enable access to Azure Resource Manager for template deployment' is checked and highlighted with a red box. Below this, there's a form for adding a new access policy, with a placeholder 'Your username' in the 'USER' field, which is also highlighted with a red box.

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 58

Drag and Drop Question

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 in sequence? To answer, move the appropriate commands from the list of commands to the answer area and arrange them in the correct order.

Commands	Answer Area
helm install	
kubectl create	▶
helm completion	◀
helm init	◀
helm serve	▶

Answer:

Commands	Answer Area
	kubectl create
	helm init
helm completion	▶
	helm install
helm serve	◀

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 59

Drag and Drop Question

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

Which type of security tool should you recommend for each stage of the development process?

To answer, drag the appropriate security tools to the correct stages. Each security tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content

NOTE: Each correct selection is worth one point.

Security Tools

Penetration testing

Static code analysis

Threat modeling

Answer Area

Pull request:

Continuous integration:

Continuous delivery:

Answer:

Security Tools

Answer Area

Pull request: Threat modeling

Continuous integration: Static code analysis

Continuous delivery: Penetration testing

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 60

Drag and Drop Question

You need to recommend project metrics for dashboards in Azure DevOps.

Which chart widgets should you recommend for each metric? To answer, drag the appropriate chart widgets to the correct metrics. Each chart widget may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Chart Widgets

Answer Area

Burndown

The elapsed time from the creation of work items to their completion:

Cycle Time

The elapsed time to complete work items once they are active:

Lead Time

The remaining work:

Velocity

Answer:

Chart Widgets**Answer Area**

The elapsed time from the creation of work items to their completion:

Lead Time

The elapsed time to complete work items once they are active:

Cycle Time**Velocity**

The remaining work:

Burndown**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 61**

Hotspot Question

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:

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.

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 62

Drag and Drop Question

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 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:

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

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 63

Drag and Drop Question

You need to configure access to Azure DevOps Agent pool 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 DevOps 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.

Roles	Answer Area
--------------	--------------------

Administrator
Reader
Service Account
User

Organization:	
Project:	

Answer:

	Roles	Answer Area
---	--------------	--------------------

Administrator
User

Organization:	Reader
Project:	Service Account

Explanation:

Box 1: Reader

Members of the Reader role can view the organization agent pool as well as agents. You typically use this to add operators that are responsible for monitoring the agents and their health.

Box 2: Service account

Members of the Service account role can use the organization agent pool to create a project agent pool in a project. If you follow the guidelines above for creating new project agent pools, you typically do not have to add any members here.

Incorrect Answers:

In addition to all the permissions given the Reader and the Service Account role, members of the administrator role can register or unregister agents from the organization agent pool. They can also refer to the organization agent pool when creating a project agent pool in a project. Finally, they can also manage membership for all roles of the organization agent pool. The user that

created the organization agent pool is automatically added to the Administrator role for that pool.

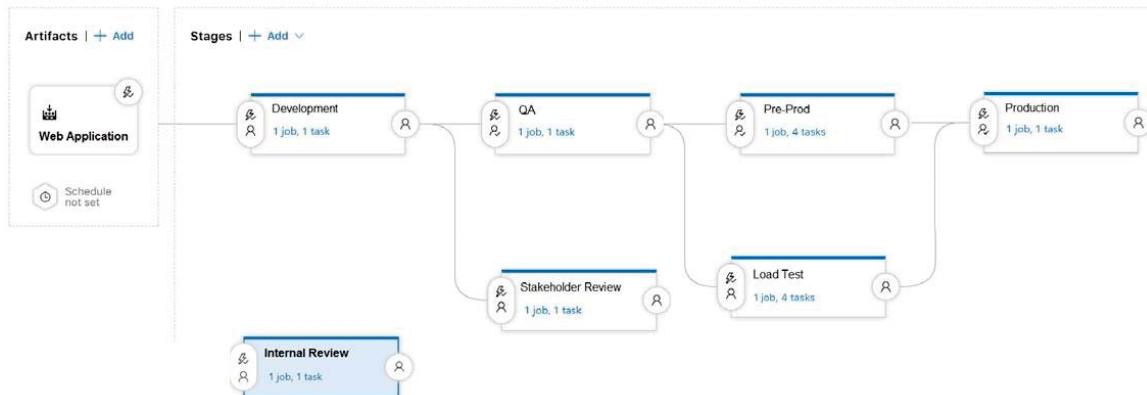
References:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues>

QUESTION 64

Hotspot Question

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 65

Drag and Drop Question

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

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

You plan to use Azure Repos for all the projects.

Which version control system should you use for each project? To answer, drag the appropriate version control systems to the correct projects. Each version control system may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Version Control Systems
Answer Area

Git

Project 1:

Perforce

Project 2:

Subversion

Project 3:

Team Foundation Version Control

Project 4:

Answer:
Version Control Systems
Answer Area

Project 1:

Team Foundation Version Control

Project 2:

Git

Project 3:

Subversion

Project 4:

Perforce

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 66

Drag and Drop Question

You are 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 built 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	Answer Area
Hosted Windows Container	
Hosted Ubuntu 1604	An application that runs on iOS:
Hosted macOS	An Internet Information Services (IIS) web application that runs in Docker:
Hosted	
Default	

Answer:

Build Agent Pools	Answer Area
Hosted Windows Container	
Hosted Ubuntu 1604	An application that runs on iOS: Hosted macOS
	An Internet Information Services (IIS) web application that runs in Docker: Hosted
Default	

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 67

Hotspot Question

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 in the answer area.
NOTE: Each correct selection is worth one point.

Groups to control the build access:

Active Directory groups
Azure Active Directory groups
Microsoft Visual Studio App Center distribution groups

Group type:

Private
Public
Shared

Answer:

Groups to control the build access:

Active Directory groups
Azure Active Directory groups
Microsoft Visual Studio App Center distribution groups

Group type:

Private
Public
Shared

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 68

Hotspot Question

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 in Azure DevOps should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Developers:

Basic
Stakeholder

Pilot users:

Basic
Stakeholder

Answer:

Developers:

Basic
Stakeholder

Pilot users:

Basic
Stakeholder

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 69

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You integrate a cloud-hosted Jenkins server and a new Azure Dev Ops deployment.

You need Azure Dev Ops to 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 70

Your company develops an app for iOS. 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 71

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

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 72

Your company is building a mobile app that targets Android devices and iOS 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: 
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 73

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: C

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 74

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

Explanation:

The options you can choose for a queuing policy are:

- Number of parallel deployments

- If you specify a maximum number of deployments, two more options appear:
 - Deploy all in sequence
 - Deploy latest and cancel the others: Use this option if you are producing releases faster than builds, and you only want to deploy the latest build.

References:

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

QUESTION 75

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 76

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

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

1. Select Repos, Files.
2. From the repo drop-down, select Import repository.
3. 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 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. PDM
- B. OWASPZAP
- C. WhiteSource
- D. Jenkins

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:

1. Detect and remedy vulnerable open source components.
2. Generate comprehensive open source inventory reports per project or build.
3. Enforce open source license compliance, including dependencies' licenses.
4. Identify outdated open source libraries with recommendations to update.

Note: Black duck would also be a good answer, but it is not an option here.

References: <https://www.azuredevopslabs.com/labs/vstsextend/WhiteSource/>

QUESTION 78

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: 

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.

Incorrect Answers:

D: YAML doesn't work with Azure pipeline deployment groups.

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/custom-script-windows>

QUESTION 79

Drag and Drop Question

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.

Files	Answer Area
The .npmrc file in the project	Feed registry information: <input type="text"/> File
The npmrc file in the user's home folder	Credentials: <input type="text"/> File
The Package.json file in the project	
The Project.json file in the project	

Answer:

Files**Answer Area**

Feed registry information: The .npmrc file in the project

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

The Package.json file in the project

The Project.json file in the project

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 80

Drag and Drop Question

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-enabled 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 correct order.

Commands
Answer Area

az role assignment create

az aks get-credentials

az aks create

az ad sp create-for-rbac

kubectl create


Answer:

Commands
Answer Area

az role assignment create

az aks create

az aks get-credentials

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 81

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result these questions will not appear in the review screen.

You integrate a cloud-hosted Jenkins server and a new Azure DevOps deployment.

You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.

Solution: You create a service hook subscription that uses the build completed event.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

QUESTION 82

Case Study 1 - Litware

Overview

Existing Environment

Litware, Inc. is 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.NET web forms that use logic written in VB.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 live 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 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.

Customers report that bug reporting is overly complex.

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 existing retirement fund management system.

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.

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

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

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

Technical requirements

The company's investment planning applications suite must meet the following 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 releases must remain available for 30 days, except for production releases, which must be kept for 60 days.
- 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 HTTPS.
- The required operating system configuration for the test servers changes weekly. Azure Automation State Configuration must be used to ensure that the operating system on each test server is configured the same way when the servers are created and checked periodically.

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 $vmaname  
-ConfigurationMode 'ApplyOnly'
```

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

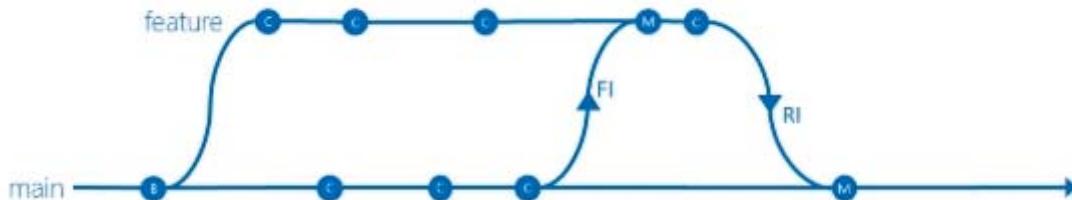
- A. release isolation
- B. main only
- C. development isolation
- D. feature isolation

Answer: D

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 83

Case Study 1 - Litware

Overview

Existing Environment

Litware, Inc. is 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.NET web forms that use logic written in VB.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 live 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 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.

Customers report that bug reporting is overly complex.

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 existing retirement fund management system.

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.

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

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

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

Technical requirements

The company's investment planning applications suite must meet the following 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 releases must remain available for 30 days, except for production releases, which must be kept for 60 days.
- 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 HTTPS.
- The required operating system configuration for the test servers changes weekly. Azure Automation State Configuration must be used to ensure that the operating system on each test server is configured the same way when the servers are created and checked periodically.

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'
```

Drag and Drop Question

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.

Access Levels

Collaborator

Contributor

Owner

Reader

Answer Area

Developers:

Team Leaders:

Answer:**Access Levels**

Collaborator

Contributor

Answer Area

Developers:

 Reader

Team Leaders:

 Owner**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				✓

QUESTION 84

Case Study 2 - Contoso, Ltd

Background

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

Contoso plans to improve its IT development and operations processes by implementing Azure 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.

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 identifies the following technical requirements:

- Implement build agents for Project1.
- Whenever possible, use Azure resources.
- Avoid using deprecated technologies.
- 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.
 - Whenever possible implement automation and minimize administrative effort.
- Implement Project3, Project5, Project6, and Project7 based on the planned changes
- Implement Project4 and configure the project to push Docker images to Azure Container Registry.

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 85

Case Study 2 - Contoso, Ltd

Background

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

Contoso plans to improve its IT development and operations processes by implementing Azure 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.

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 identifies the following technical requirements:

- Implement build agents for Project1.
- Whenever possible, use Azure resources.
- Avoid using deprecated technologies.
- 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.
- Whenever possible implement automation and minimize administrative effort.
- Implement Project3, Project5, Project6, and Project7 based on the planned changes
- Implement Project4 and configure the project to push Docker images to Azure Container Registry.

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	Answer Area
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:

Actions	Answer Area
	Create a repository
Add a build policy for the fork.	Add a build policy for the master branch.
	Create a branch.
Add an application access policy.	
Create a fork.	

Explanation:

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.

Step 1: Create a repository

Step 2: Add a build policy for the master branch

Step 3: Create a branch

Each branch must have a defined policy about how to integrate code into this branch.

References:

<https://docs.microsoft.com/en-us/azure/devops/learn/devops-at-microsoft/release-flow>

QUESTION 86

Case Study 2 - Contoso, Ltd

Background

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

Contoso plans to improve its IT development and operations processes by implementing Azure 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.

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 identifies the following technical requirements:

- Implement build agents for Project1.

- Whenever possible, use Azure resources.
- Avoid using deprecated technologies.
- 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.
- Whenever possible implement automation and minimize administrative effort.
- Implement Project3, Project5, Project6, and Project7 based on the planned changes
- Implement Project4 and configure the project to push Docker images to Azure Container Registry.

Drag and Drop Question

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.

Actions	Answer Area
Sign in to Azure DevOps by using an account that is assigned the Administrator service connection security role.	
Install the Azure Pipelines agent on on-premises virtual machine.	
Create a personal access token in the Azure DevOps organization of Contoso.	
Install and register the Azure Pipelines agent on an Azure virtual machine.	
Sign in to Azure DevOps by using an account that is assigned the agent pool administrator role.	

Answer:

Actions	Answer Area
	Sign in to Azure DevOps by using an account that is assigned the Administrator service connection security role.
Install the Azure Pipelines agent on on-premises virtual machine.	Create a personal access token in the Azure DevOps organization of Contoso.
	Install and register the Azure Pipelines agent on an Azure virtual machine.

Sign in to Azure DevOps by using an account that is assigned the agent pool administrator role.

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/>

Question Set 3

QUESTION 87

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 88

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 89

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 90

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 91

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 92

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 93

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 94

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: C

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 95

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 96

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 97

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: E

Explanation:

The Microsoft-hosted agent pool provides 7 virtual machine images to choose from:

Ubuntu 16.04 (ubuntu-16.04)

Windows Server 1803 (win1803) -for running Windows containers

Visual Studio 2019 Preview on Windows Server 2019 (windows-2019)

Visual Studio 2017 on Windows Server 2016 (vs2017-win2016)

Visual Studio 2015 on Windows Server 2012R2 (vs2015-win2012r2)

macOS X Mojave 10.14 (macOS-10.14)

macOS X High Sierra 10.13 (macOS-10.13)

References:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/hosted?view=azure-devops>

QUESTION 98

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 99

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 100

Drag and Drop Question

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.

Processes	Answer Area
Agile	Litware
CMMI	Contoso:
Scrum	A. Datum:
XP	

Answer:

Processes	Answer Area
	Litware
	Contoso:
	A. Datum:
XP	Scrum
	Agile
	CMMI

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 101

Hotspot Question

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.

Answer Area

```
{  
    "policyRule": {  
        "if": {  
            "allOf": [  
                {  
                    "field": "type",  
                    "equals":  
                        ,  
                        {  
                            "MicrosoftResources/deployments"  
                            "MicrosoftResources/subscriptions"  
                            "MicrosoftResources/subscriptions/resourceGroups"  
                        }  
                },  
                {  
                    "not": {  
                        "field": "tags['organization']",  
                        "equals": "Contoso"  
                    }  
                }  
            ]  
        },  
        "then": {  
            "effect":  
                "details": [  
                    "Append",  
                    "Deny",  
                    "DeployIfNotExists",  
                {  
                    "field": "tags['organization']",  
                    "value": "Contoso"  
                }  
            ]  
        }  
    }  
}
```

Answer:

Answer Area

```
{
    "policyRule": {
        "if": {
            "allOf": [
                {
                    "field": "type",
                    "equals":
                        ,
                }
            ],
            "not": {
                "field": "tags['organization']",
                "equals": "Contoso"
            }
        }
    },
    "then": {
        "effect": "Append",
        "details": [
            "Deny",
            "DeployIfNotExists",
        ]
    }
}
}
```

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 102

Drag and Drop Question

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.

Release Strategies

- Blue/Green deployment
- Canary deployment
- Rolling deployment

Answer Area:

App1:	<input type="text"/>
App2:	<input type="text"/>

Answer:

Release Strategies**Blue/Green deployment****Answer Area:**

App1: Canary deployment

App2: Rolling deployment

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 103

Drag and Drop Question

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	Answer Area
Assembla Subversion	Project1:
Bitbucket Cloud	Project2:
Git in Azure Repos	Project3:
GitHub Enterprise	

Answer:

Version Control Systems	Answer Area
Assembla Subversion	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 Bitbucket 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 104

Drag and Drop Question

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.

Commands**Answer Area**

helm install

kubectl create



helm completion



helm init

helm serve

Answer:

Commands**Answer Area**

kubectl create

helm init



helm completion



helm install



helm serve

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 105

Drag and Drop Question

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.

Actions Commands Cmdlets Statements	Answer Area
Run Code Analysis	
Visual Studio Test	
Publish Build Artifacts	
Visual Studio Build	
Prepare Analysis Configuration	

Answer:

Actions Commands Cmdlets Statements	Answer Area
	Prepare Analysis Configuration
	Visual Studio Build
Publish Build Artifacts	Visual Studio Test
	Run Code Analysis

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

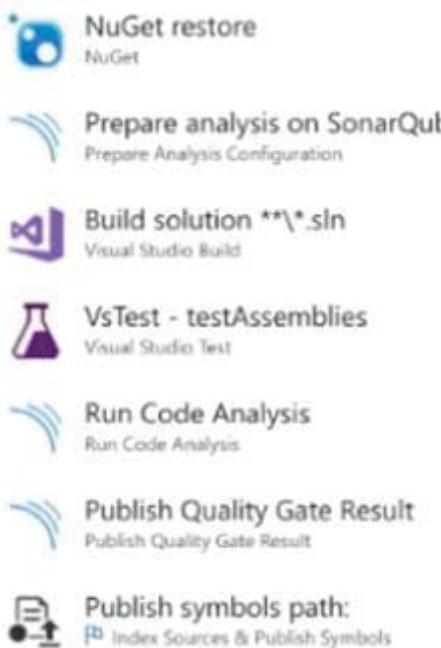
Reorder the tasks to respect the following order:

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>

QUESTION 106

Hotspot Question

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.

Answer Area

JIRA:

Boards
Build pipelines
Release pipelines
Repos

Jenkins:

Boards
Build pipelines
Release pipelines
Repos

Octopus:

Boards
Build pipelines
Release pipelines
Repos

Answer:

Answer Area

JIRA:

Boards
Build pipelines
Release pipelines
Repos

Jenkins:

Boards
Build pipelines
Release pipelines
Repos

Octopus:

Boards
Build pipelines
Release pipelines
Repos

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 107**

Drag and Drop Question

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.

Actions	Answer Area
Group the related components.	
Assign ownership to each component group.	
Create a dependency graph for the application.	
Identify the most common language used.	
Rewrite the components in the most common language.	

Answer:

Actions	Answer Area
	Create a dependency graph for the application.
	Group the related components.
	Assign ownership to each component group.
Identify the most common language used.	
Rewrite the components in the most common language.	

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/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 108

Drag and Drop Question

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.

Tools	Answer Area
Impact	Feature usage:
User Flows	User actions by day:
Users	The effect that the performance of the application has on the usage of a page or a feature:

Answer: 

Tools	Answer Area
	Feature usage:
	User actions by day:
	The effect that the performance of the application has on the usage of a page or a feature:

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 109

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: 

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 110

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: 

Explanation:

Instead use Octopus Tentacle.

References:

<https://explore.emtecinc.com/blog/octopus-for-automated-deployment-in-devops-models>

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 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 112

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 113

SIMULATION

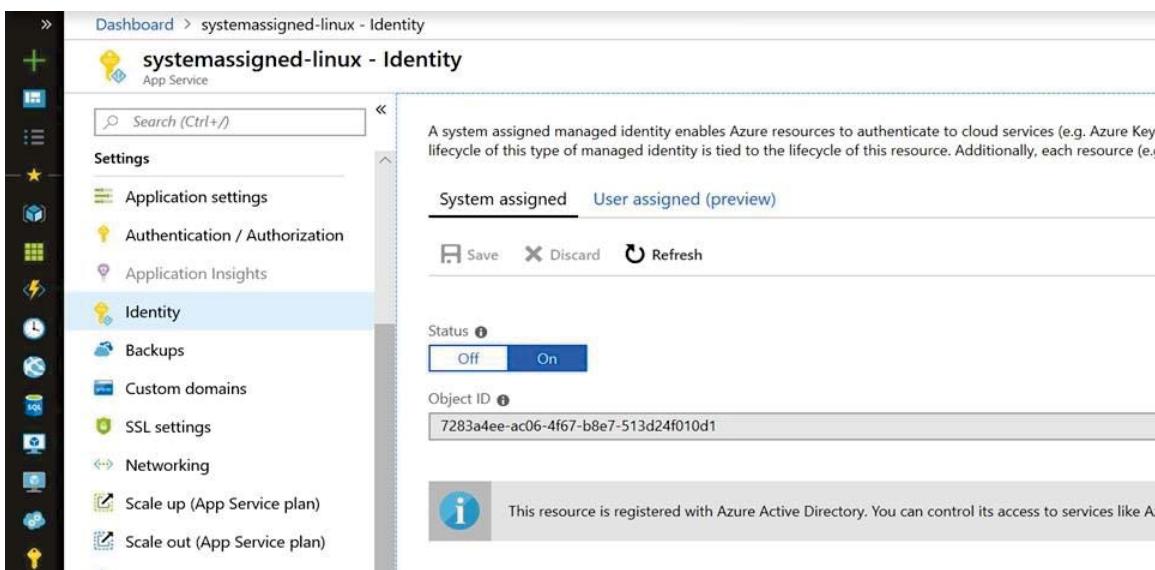
You need to ensure that an Azure web app named az400-9940427-main can retrieve secrets from an Azure key vault named az400-9940427-kv1 by using a system managed identity.

The solution must use the principle of least privilege.

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

Answer:

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.



The screenshot shows the Azure portal interface for managing an App Service. The left sidebar has a 'System assigned' icon. The main area shows the 'Identity' settings for the 'systemassigned-linux' app service. The 'System assigned' tab is selected, and the status is set to 'On'. A note at the bottom states: 'This resource is registered with Azure Active Directory. You can control its access to services like AAD Connect, Key Vault, and more.' There are also 'Save', 'Discard', and 'Refresh' buttons.

References:

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

QUESTION 114

SIMULATION

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:

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 115

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 116

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 117

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: 

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 118

SIMULATION

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:

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.

my-demo-app - Deployment slots

App Service

Search (Ctrl+ /)

Save Discard Swap Refresh

Add Slot

You haven't added any deployment slots. Click here to get started.

Deployment Slots

Deployment slots are live apps with their own hostnames. App content and configurations elements can be swapped between two deployment slots, including the production slot.

NAME	STATUS	APP SERVICE PLAN	TRAFFIC %
my-demo-app PRODUCTION	Running	myAppServicePlan	100

Deployment slots

Quickstart

Deployment Center

Settings

Configuration

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.

Add a slot

Name
staging

Clone settings from:
Do not clone settings

Add **Close**

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.

my-demo-app - Deployment slots

Deployment Slots

Deployment slots are live apps with their own hostnames. App content and configurations elements can be swapped between two deployment slots, including the production slot.

NAME	STATUS	APP SERVICE PLAN	TRAFFIC %
my-demo-app PRODUCTION	Running	myAppServicePlan	100
my-demo-app-staging	Running	myAppServicePlan	0

6. Change TRAFFIC % to 10

References:

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

QUESTION 119 SIMULATION

You plan to store signed images in an Azure Container Registry instance named az4009940427acr1.

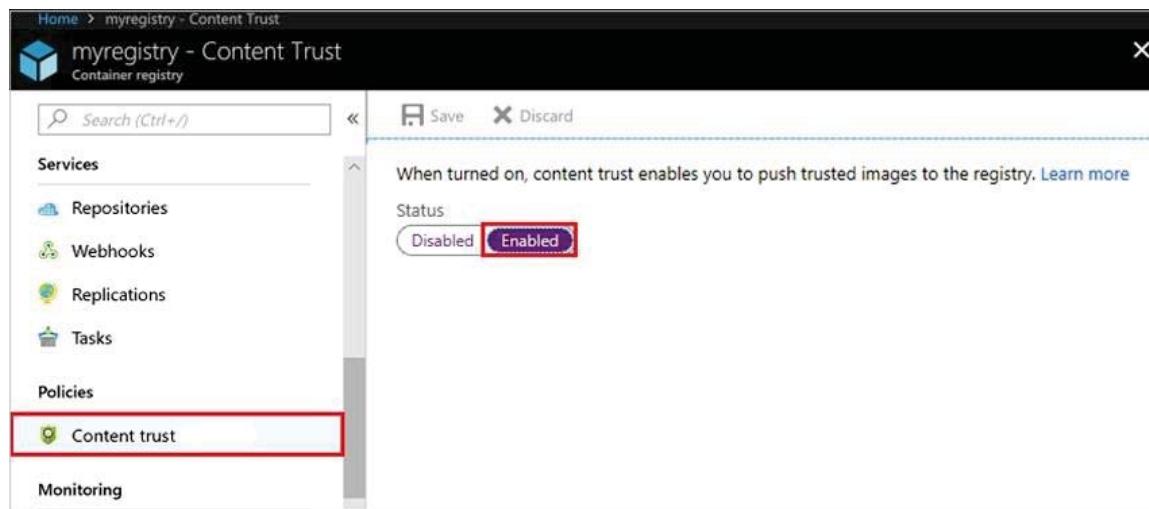
You need to modify the SKU for az4009940427acr1 to support the planned images. The solution must minimize costs.

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

Answer:

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 120
SIMULATION

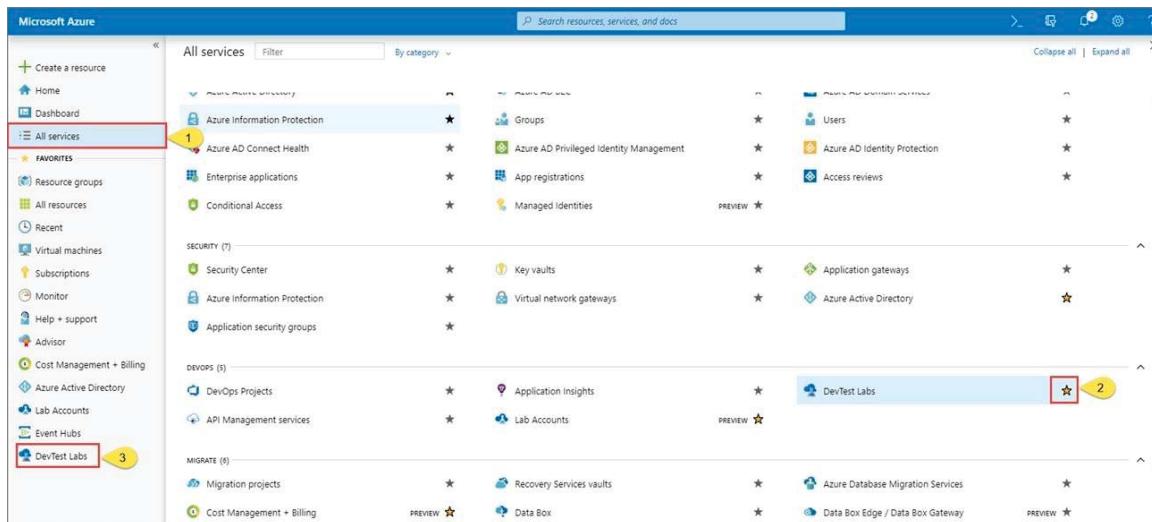
You need to create a virtual machine template in an Azure DevTest Labs environment named az400-9940427-dtl1. The template must be based on Windows Server 2016 Datacenter. Virtual machines created from the template must include the selenium tool and the Google Chrome browser.

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

Answer:

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-cyrillic/azure/lab-services/devtest-lab-vm-powershell>

QUESTION 121

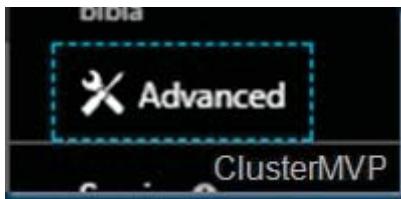
SIMULATION

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:

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://robertsmmit.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 122

SIMULATION

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:

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.

Microsoft Azure Stack - Administration

Home > New > Custom deployment

Custom deployment
Deploy from a custom template

Template
Edit template

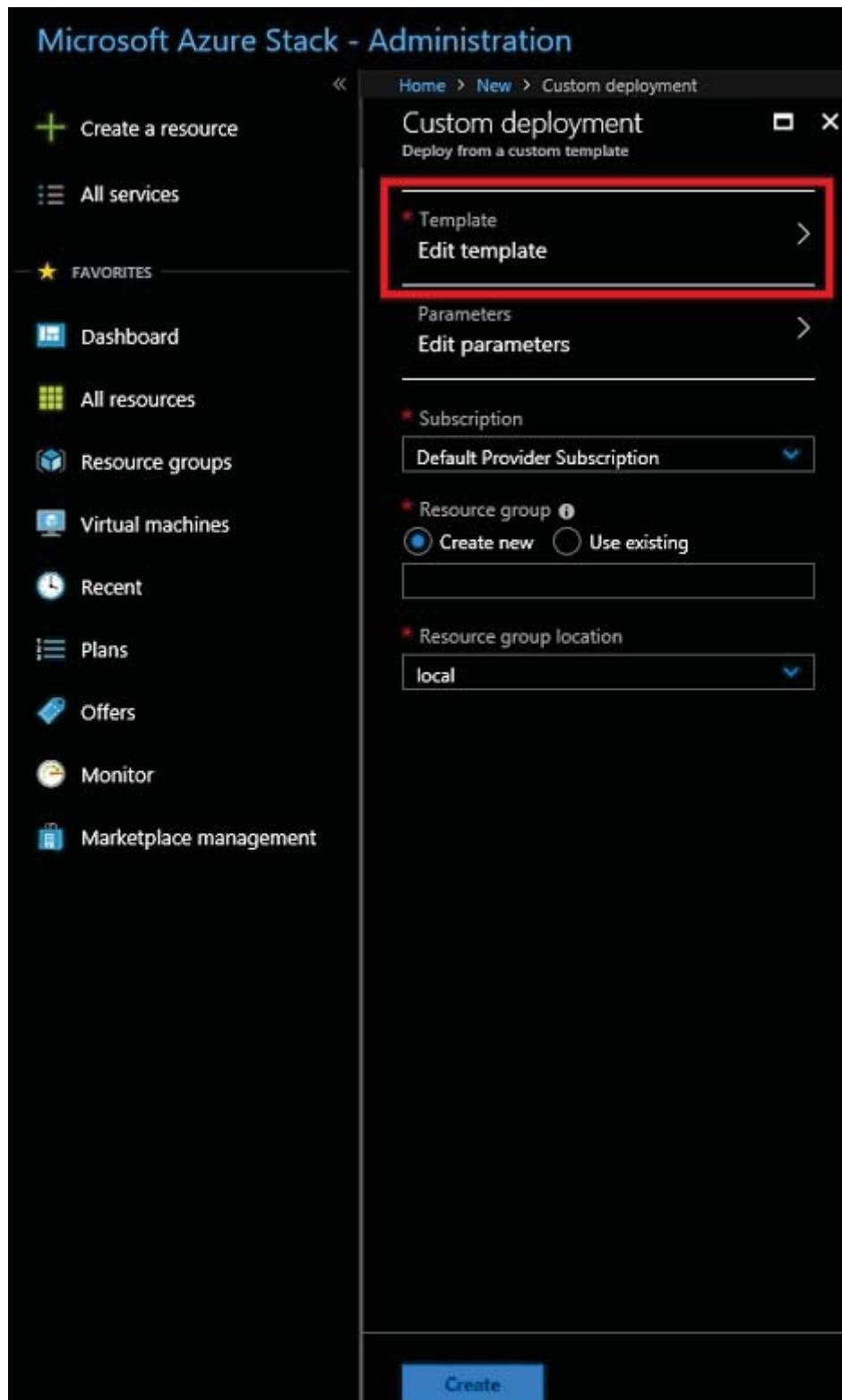
Parameters
Edit parameters

Subscription
Default Provider Subscription

Resource group
 Create new Use existing

Resource group location
local

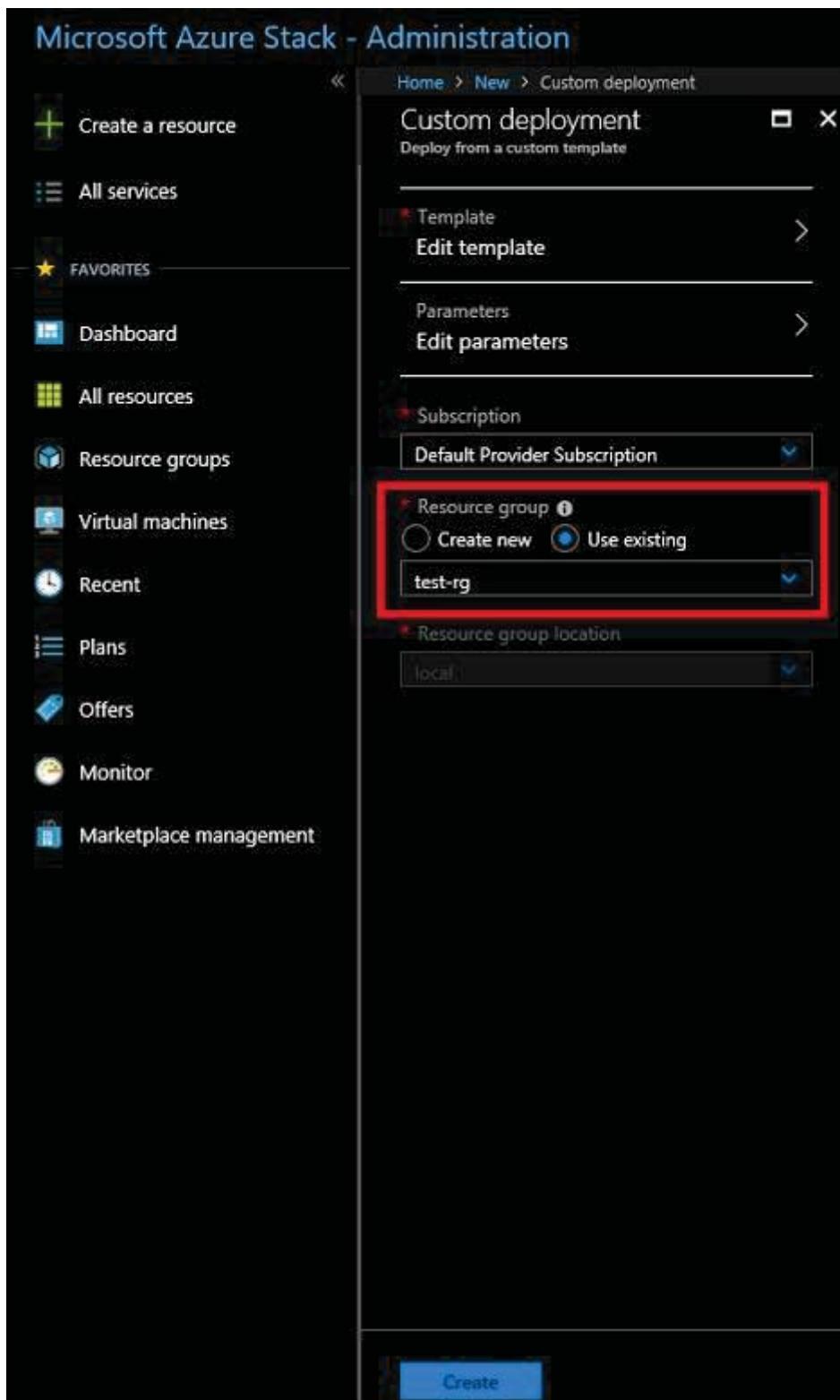
Create



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 123

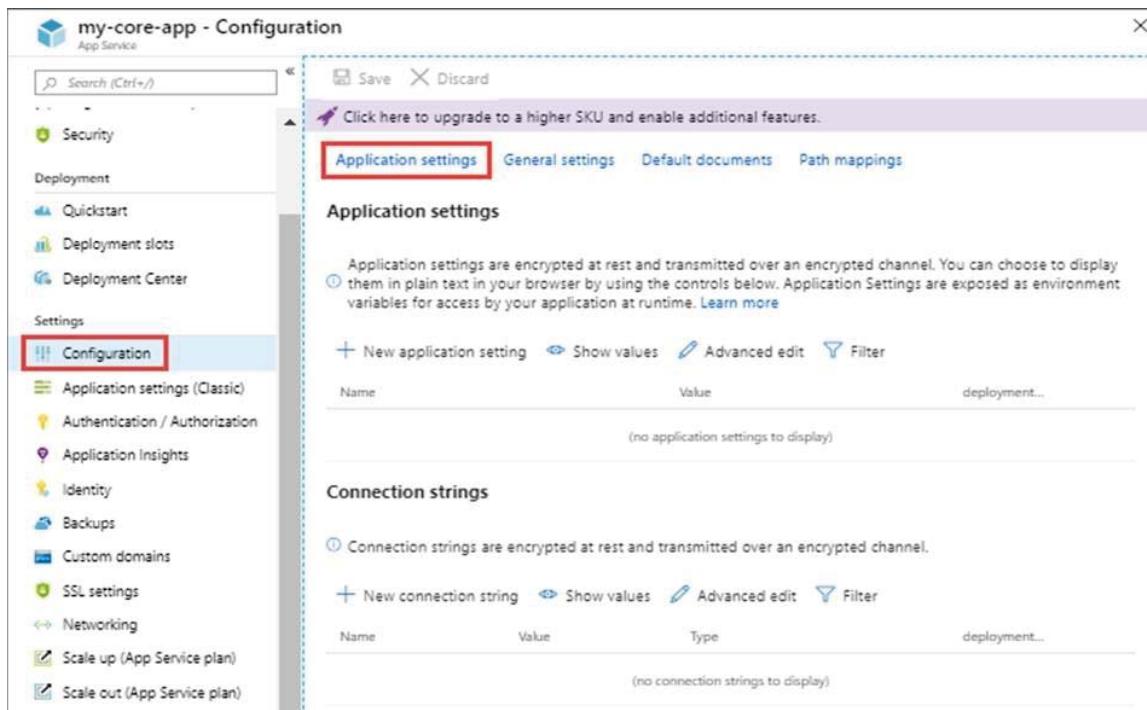
SIMULATION

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:

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.



The screenshot shows the Azure portal's configuration interface for an App Service named 'my-core-app'. The left sidebar lists various configuration sections like Security, Deployment, and Settings, with 'Configuration' being the active tab. Under 'Application settings', there is a table with one entry: Name: MAX_ITEMS, Value: 50. The 'Connection strings' section below is currently empty.

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 124

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: B 

QUESTION 125

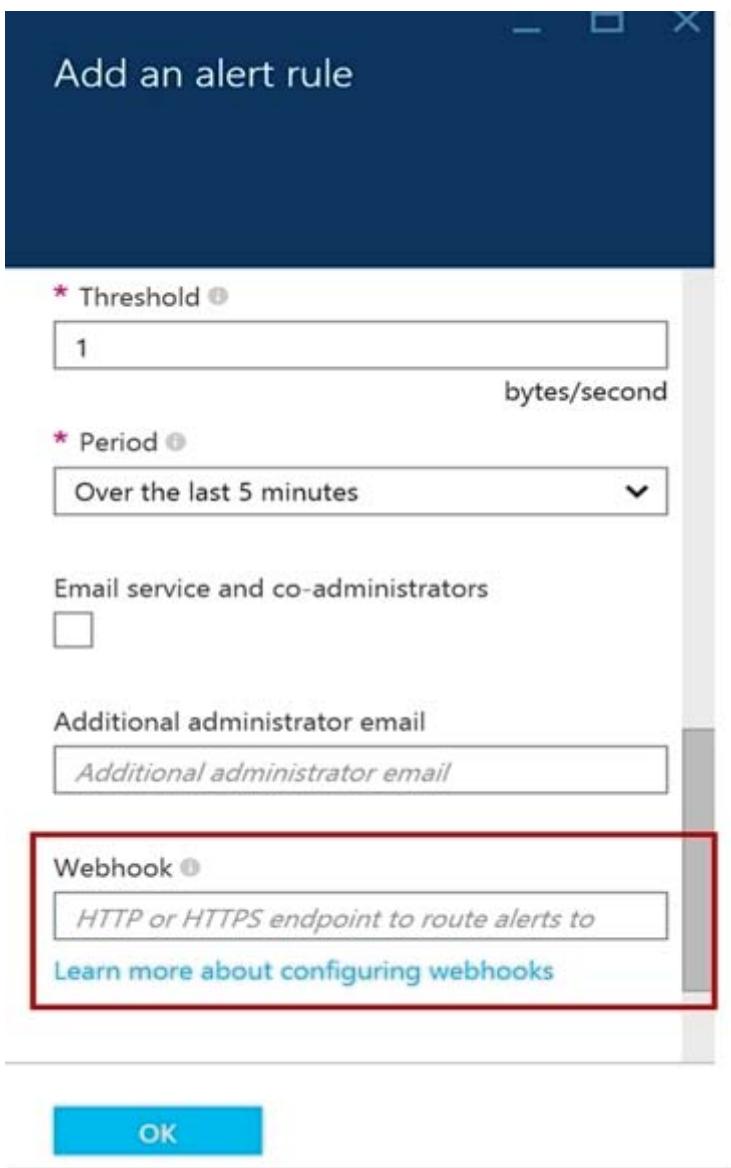
SIMULATION

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:

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 126
SIMULATION

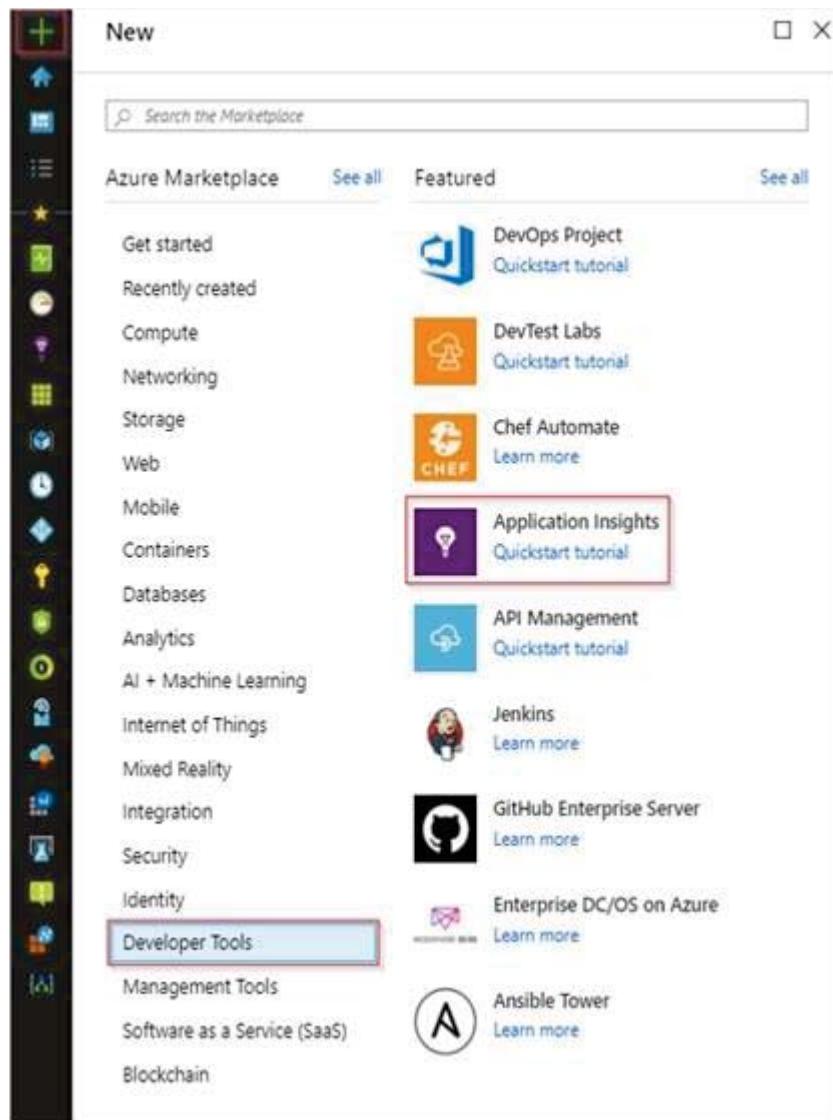
You need to create an instance of Azure Application Insights named az400-9940427-main and configure the instance to receive telemetry data from an Azure web app named az400-9940427-main.

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

Answer:

- 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.

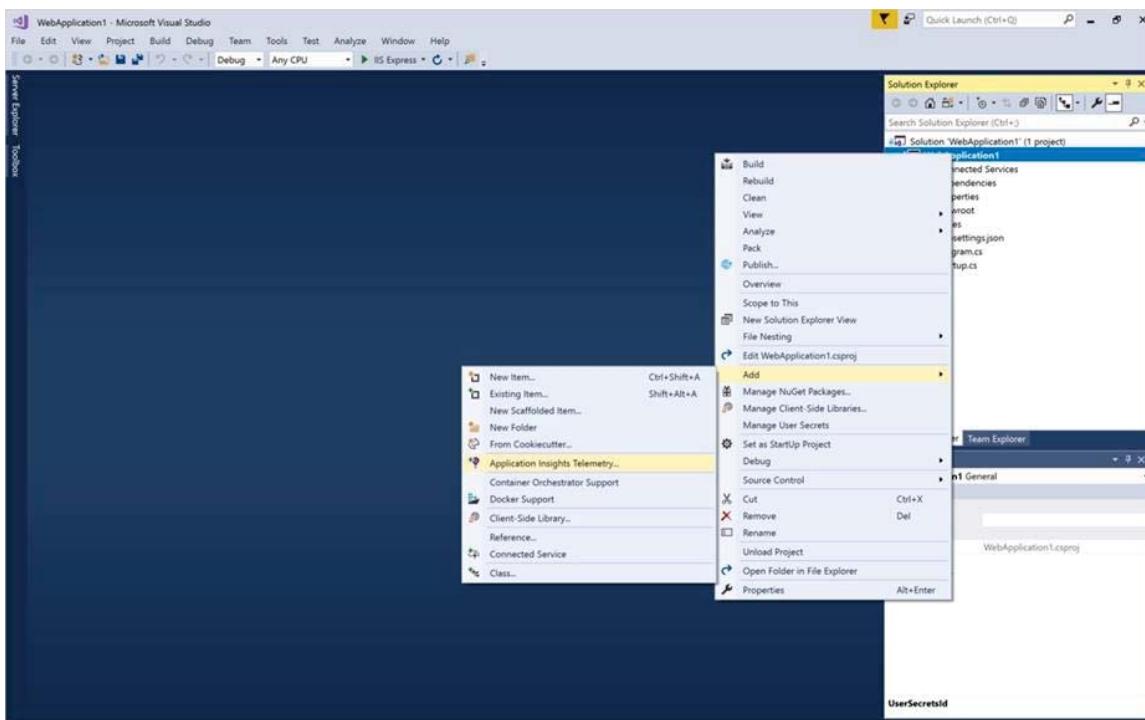


3. Enter the following settings, and then select Review + create.

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/en-us/bs-latn-ba/azure/azure-monitor/learn/dotnetcore-quick-start?view=vs-2017>

QUESTION 127

Drag and Drop Question

Your company has a project in Azure DevOps.

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

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

What should you include in the recommendation? To answer, drag the appropriate configurations to the correct targets. Each configuration may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Configurations**Answer Area**

an Azure Key Vault access policy

Restrict access to delete the key vault:

a personal access token (PAT)

Restrict access to the secrets in Key Vault by using:

RBAC

Answer: **Configurations****Answer Area**

an Azure Key Vault access policy

Restrict access to delete the key vault: RBAC

a personal access token (PAT)

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

RBAC

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 128**

Drag and Drop Question

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.

Actions**Answer Area**

Create a new Azure Artifacts feed.

Configure a self-hosted agent.

Publish a package.



Install a package.

Connect to an Azure Artifacts feed.

Answer:**Actions****Answer Area**

Configure a self-hosted agent.

Create a new Azure Artifacts feed.



Install a package.

Connect to an Azure Artifacts feed.

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 129**

Hotspot Question

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 Area

Object to create:

A build task
A deployment task
An artifacts repository

Service to use:

WhiteSource Bolt
Bamboo
CMake
Chef

Answer:

Answer Area

Object to create:

A build task
A deployment task
An artifacts repository

Service to use:

WhiteSource Bolt
Bamboo
CMake
Chef

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.

1. Go to Builds section under Pipelines tab, select the build definition WhiteSourceBolt and click on Queue to trigger a build.
2. 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 130

Case Study 1 - Litware

Overview

Existing Environment

Litware, Inc. is 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.NET web forms that use logic written in VB.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 live 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 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.

Customers report that bug reporting is overly complex.

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 existing retirement fund management system.

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.

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

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

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

Technical requirements

The company's investment planning applications suite must meet the following 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 releases must remain available for 30 days, except for production releases, which must be kept for 60 days.
- 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 HTTPS.
- The required operating system configuration for the test servers changes weekly. Azure Automation State Configuration must be used to ensure that the operating system on each test server is configured the same way when the servers are created and checked periodically.

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 $vmaname  
-ConfigurationMode 'ApplyOnly'
```

Hotspot Question

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 Area**Build agent:**

- A hosted service
- A source control system
- The developers' computers

Release agent:

- A hosted service
- A source control system
- The developers' computers

Answer:

Answer Area

Build agent:

- A hosted service
- A source control system**
- The developers' computers

Release agent:

- A hosted service**
- A source control system
- The developers' computers

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 131

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 132

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: B**Explanation:**

Instead use Octopus Tentacle.

Reference:

<https://explore.emtecinc.com/blog/octopus-for-automated-deployment-in-devops-models>

QUESTION 133

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 134

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 135

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 136

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 137

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 138

Drag and Drop Question

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 Area

Private

Public

Shared

Group1:

Group2:

Group3:

Answer:

Answer Area

Group1: Private

Group2: Public

Group3: Shared

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 139**SIMULATION**

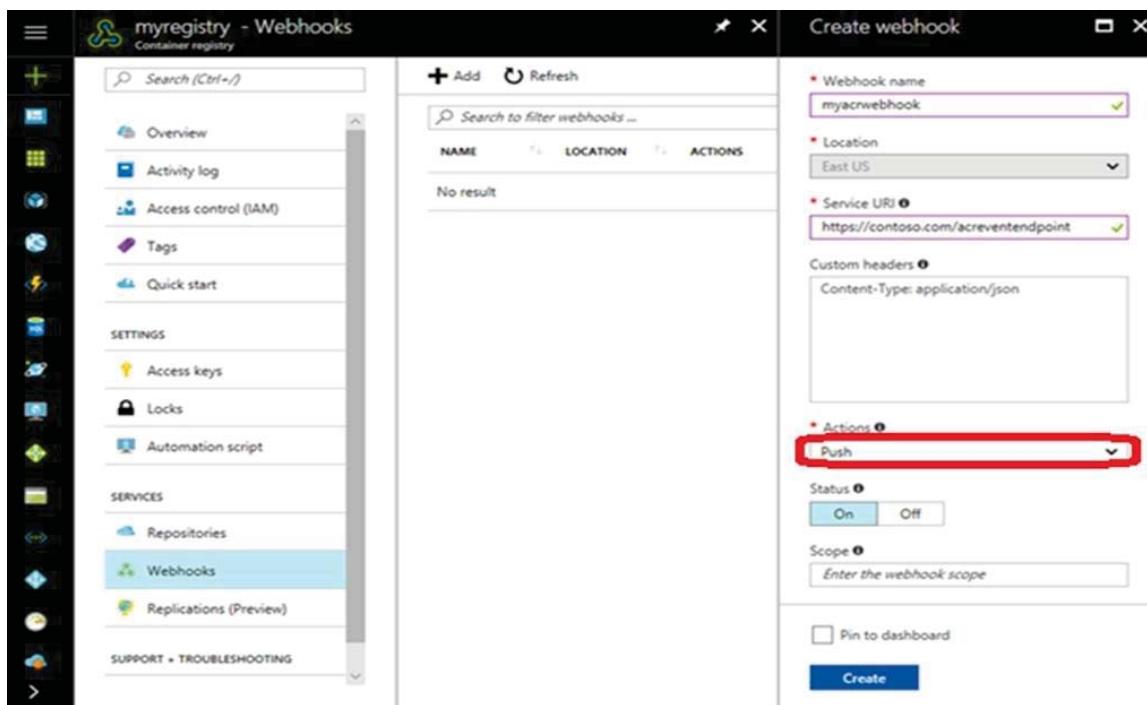
You need to ensure that the https://contoso.com/statushook webhook is called every time a repository named az40010480345acr1 receives a new version of an image named dotnetapp.

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

Answer:

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

Example web hook:



Reference:

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

QUESTION 140

A team currently makes use of Docker containers for building their application. The application lifecycle also makes use of Azure Devops. Exploits need to be detected in the Docker images before the container can be used. These exploits must be detected as early on in the lifecycle as possible.

Which of the following would you configure as part of the lifecycle?

- A. Ensure a scheduled task runs against the production container in the continuous deployment pipeline
- B. Ensure a scheduled task runs against the staging container in the continuous deployment pipeline

- C. Ensure a scheduled task runs against the image registry to analyse the images
- D. Run manual tasks to analyse the docker containers in the planning phase

Answer: C

Explanation:

It's always good to have an on-going process to analyse the images in the image registry itself. There are some points also given in a whitepaper which relates to security for containers

[Scan for vulnerabilities before pushing images to the registry](#)

A container image registry is a service that stores container images and is hosted either by a partner or as a public/private registry such as DockerHub and Quay.

As a final check after container development is complete, you should perform a vulnerability scan on containers before pushing the images to the registry.

[Continue scanning in the registry](#)

New vulnerabilities are discovered all the time, so scanning for and identifying vulnerabilities is a continuous process. Continue to scan container images in the registry both to identify any flaws that were somehow missed during development and to address any newly discovered vulnerabilities that might exist in the code used in the container images.

Options A and B are incorrect since this would be too late to detect issues in the application lifecycle.

Option D is incorrect because it is inefficient to use manual processes.

<https://azure.microsoft.com/en-us/resources/container-security-in-microsoft-azure/en-us/>

QUESTION 141

A team is currently using a project in Azure Devops. The team needs to have a policy in place that ensures the following:

- A user should be able to merge to a master branch even if the code fails to compile.

The solution must use the principle of least privilege.

Which of the following would you implement?

- A. Ensure that the user is added to the Build Administrators group
- B. Ensure that the user is added to the Project Administrators group
- C. Ensure to modify the access control for the user from the security setting of the repository
- D. Ensure to modify the access control for the user from the security setting of the branch

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-permissions?view=azure-devops>

QUESTION 142

A team has the following DockerFile that will create an image FROM windowsservercore

```
RUN powershell.exe -Command Invoke-WebRequest  
"https://www.python.org/ftp/python/3.5.1/python-3.5.1.exe" -OutFile c:\python-3.5.1.exe  
RUN powershell.exe -Command Start-Process c:\python-3.5.1.exe -ArgumentList '/quiet  
InstallAllUsers=1 PrependPath=1' -Wait
```

RUN powershell.exe -Command Remove-Item c:\python-3.5.1.exe -Force

You need to ensure that you optimize the DockerFile. Which of the following can you do to create an optimized DockerFile?

- A. Change the base image
- B. Place an ENTRYPOINT
- C. Ensure to have only one RUN command
- D. Create a working directory

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/virtualization/windowscontainers/manage-docker/optimize-windows-dockerfile>

QUESTION 143

A project team is using Azure Devops for building and deploying projects using pipelines. The application using this infrastructure is a Java based application.

You need to ensure a strategy is in place for managing technical debt.

Which of the following would you recommend? (Choose 2)

- A. Carry out an integration between Azure Devops and Azure DevTest Labs
- B. Carry out an integration between Azure Devops and SonarQube
- C. Ensure to configure post-deployment approvals in the deployment pipeline
- D. Ensure to configure pre-deployment approvals in the deployment pipeline

Answer: BD

Explanation:

SonarQube is the perfect tool that can be used for measuring technical debt.

About SonarQube

[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.

Then ensure to create a pre-deployment approval task so that the approver can view the technical debt before proceeding with the approval.

Option A is incorrect because Azure DevTest Labs cannot provide information on technical debt. Option C is incorrect because you need to ensure the reviewer can review the technical debt first.
<https://docs.microsoft.com/en-us/azure/devops/java/sonarqube?view=azure-devops>

QUESTION 144

A company is currently using Team Foundation Server 2013. They want to now migrate to Azure Devops. Below are the key points that need to be observed for the migration

- All dates for the Team Foundation Version Control changesets need to be preserved
- All TFS artifacts need to be migrated
- The migration effort should be minimized

Which of the following step needs to be performed on the Team Foundation Server?

- A. The TFS Java SDK needs to be installed.
- B. The latest .Net framework needs to be installed.
- C. The latest powershell version needs to be installed.
- D. The TFS server needs to be upgraded to the latest RTW release

Answer: D

Explanation:

In the whitepaper showcasing how to migrate from TFS to Azure Devops , there is a section which states that the TFS server needs to be migrated to the latest version. This would help ensure that the TFS schema is close to the one represented in Azure Devops services.
<https://azure.microsoft.com/en-us/services/devops/migrate/>

QUESTION 145

A team currently has the source code repository defined in Github. They want to now migrate their code onto Azure Devops. Which of the following step could be used to clone the repository from Github to Azure Devops?

- A. Implement a new pull request
- B. Implement a new push request
- C. Create a service hook in GitHub
- D. Choose Import from the Git repository

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/import-git-repository?view=azure-devops>

QUESTION 146

A company is currently planning on setting up Jenkins on an Azure virtual machine. Code will be build using the Jenkins server and then deployed to a Kubernetes cluster in Azure. The code will be picked up from the Azure container registry.

Which of the following needs to be implemented to ensure traffic can flow into the Jenkins instance on the Azure virtual machine

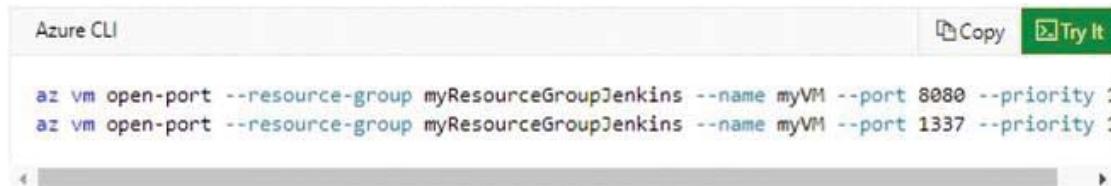
- A. Open the port 8080 on the server
- B. Add a subnet to the network
- C. Add an additional network interface to the virtual machine
- D. Implement virtual network peering

Answer: A

Explanation:

You need to ensure port 8080 is open on the virtual machine.

To allow web traffic to reach your VM, use `az vm open-port` to open port 8080 for Jenkins traffic and port 1337 for the Node.js app that is used to run a sample app:



```
Azure CLI
az vm open-port --resource-group myResourceGroupJenkins --name myVM --port 8080 --priority 1
az vm open-port --resource-group myResourceGroupJenkins --name myVM --port 1337 --priority 1
```

<https://docs.microsoft.com/en-us/azure/aks/jenkins-continuous-deployment>

QUESTION 147

A company currently uses ServiceNow for Incident and Change Management. Most of their web-based applications which are developed in-house are hosted in Azure. The company needs to ensure that whenever there is an issue in the application a ticket is generated. Which of the following can help achieve this?

- A. IT Service Management connector in Azure Log Analytics
- B. Service hooks in Azure Functions
- C. Service hooks in Azure Logic Apps
- D. Web hooks in Azure Monitor

Answer: A

Explanation:

This can be done with the help of the IT Service Management connector in Azure Log Analytics.
<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/itsmc-overview>

QUESTION 148

A team is developing an application that is based on the .Net core framework. The application will connect to a Microsoft SQL Server database. During the development stage the application will be developed using on-premise servers. For the production environment, the application will be moved to Azure and use the Azure Web App Service.

During the production stage, where should you store the database connection settings?

- A. In the Web.config file
- B. In the connection strings in the App Service
- C. In the Authentication/Authorization section in the App Service
- D. In the Identity section in the App Service

Answer: B

Explanation:

You should place this in the connection strings setting in the Azure Web App.
Option A is incorrect since this is not the recommended place to keep the database connecting string settings.
Option C is incorrect since this is used when the application needs to authenticate using external identity provider.
Option D is incorrect since this is used to authenticate to other resources in Azure.
<https://docs.microsoft.com/en-us/azure/app-service/configure-common>

QUESTION 149

A company wants to implement a package management solution for their Node.js applications. They want to ensure that developers can use their IDE to connect to the repository securely.

Which of the following would contain the credentials to connect to the package management solution?

- A. In the package.json files in the project
- B. In the project.json files in the project
- C. In the .npmrc file in the project
- D. In the .npmrc file in the user's home folder

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/devops/artifacts/npm/npmrc?view=azure-devops&tabs=windows>

QUESTION 150

A team is currently using the Azure Pipeline service for the CI/CD process for an application. The Pipeline needs to make use of a secret that needs to be shared across the pipeline. How would you define the secret?

- A. In the YAML file, add a secret variable
- B. In the YAML file, add a normal variable
- C. Set the secret in the pipeline editor
- D. Set the secret in the application

Answer: C

Explanation:

The ideal approach is to set the variable in the editor.

<https://docs.microsoft.com/en-us/azure/devops/pipelines/process/variables>

QUESTION 151

A company is currently planning on using the Azure Devops service for managing the CI/CD pipeline for various applications. The team wants to have an effective communication tool that can be used across the project. The tool should integrate with Azure Devops and also have a separation of channels for each team.

You decide to implement Bamboo?

Does this fulfil the requirement?

- A. Yes
- B. No

Answer: B

Explanation:

This is a CI/CD tool from a company called Atlassian.

<https://www.atlassian.com/software/bamboo>

QUESTION 152

A team is currently using Azure Devops for a Java based project. They need to use a static code analysis tool for the java project. Which of the following are tools that can be used along with Azure Devops for this purpose?

- A. PMD
- B. Bamboo
- C. FindBugs
- D. Jenkins

Answer: AC

Explanation:

You can use tools such as PMD and FindBugs along with Azure Devops for static code analysis.
<https://docs.microsoft.com/en-us/azure/devops/java/standalone-tools?view=azure-devops>

QUESTION 153

A team wants to implement Azure Automation DSC for a set of servers. They have currently defined the following configuration:

```
configuration TestConfig {
    Node WebServer {
        WindowsFeature IIS {
            Ensure      = 'Present'
            Name        = 'Web-Server'
            IncludeAllSubFeature = $true
        }
    }
}
```

To upload the configuration into your Automation account, which PowerShell cmdLet should we execute?

- A. Run the Start-AzureRmAutomationDscCompilationJob powershell command
- B. Run the Import-AzureRmAutomationDscConfiguration powershell command
- C. Run the Register-AzureRmAutomationDscNode powershell command
- D. Run the Get-AzureRmAutomationDscNode powershell command

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/automation/tutorial-configure-servers-desired-state>

QUESTION 154

A team needs to create a Kubernetes cluster using the Azure CLI. The Kubernetes cluster needs to have monitoring enabled.

```
az Slot1 create --name whizlab-rg --location eastus

az Slot2 create \
--resource-group whizlab-rg \
--name whizlabcluster \
--node-count 2 \
--enable-addons Slot3 \
--generate-ssh-keys
```

Which of the following would go into Slot2?

- A. group
- B. aks
- C. monitoring
- D. template

Answer: B

Explanation:

Create AKS cluster

Use the [az aks create](#) command to create an AKS cluster. The following example creates a cluster named *myAKSCluster* with one node. Azure Monitor for containers is also enabled using the *--enable-addons monitoring* parameter.

```
Azure CLI Copy Try It
az aks create \
--resource-group myResourceGroup \
--name myAKSCluster \
--node-count 1 \
--enable-addons monitoring \
--generate-ssh-keys
```

After a few minutes, the command completes and returns JSON-formatted information about the cluster.

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough>

QUESTION 155

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

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 156

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You integrate a cloud-hosted Jenkins server and a new Azure DevOps deployment.

You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.

Solution: You create a service hook subscription that uses the 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 157

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 158

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 Triggers tab of the build pipeline, you select Batch changes while a build is in progress.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead, In Visual Designer you enable continuous integration (CI) by:

1. Select the Triggers tab.
2. Enable Continuous integration.

Note: Batch changes

Select this check box if you have many 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/get-started-designer>

QUESTION 159

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

Explanation:

Technical Debt is the estimated cost to fix code elements issues.

Technical Debt Ratio: Ratio between the cost to develop the software and the cost to fix it. The Technical Debt Ratio formula is:

Remediation cost / Development cost

Which can be restated as:

Remediation cost / (Cost to develop 1 line of code * Number of lines of code) References:

<http://www.azure365.co.in/devops/3PDevOps-4>

QUESTION 160

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 161

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 162

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: 

Explanation:

B: Follow these steps to register the devices:

Select the Register devices button.

A dialog prompts for your username and password used in the Apple Developer portal.

Once you sign in with your Apple username and password, App Center adds the unprovisioned devices to both your Apple developer account and the releases provisioning profile.

Optionally you can upload a .p12 file to re-sign the app and distribute it to the newly added devices. Read more on how to generate a .p12 file.

F: Registering a device means making it part of the list of devices on the Apple Developer portal that can then be included in a provisioning profile.

Incorrect Answers:

C: Only register the application in the iTunes store when it is ready for public release.

References:

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

QUESTION 163

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.

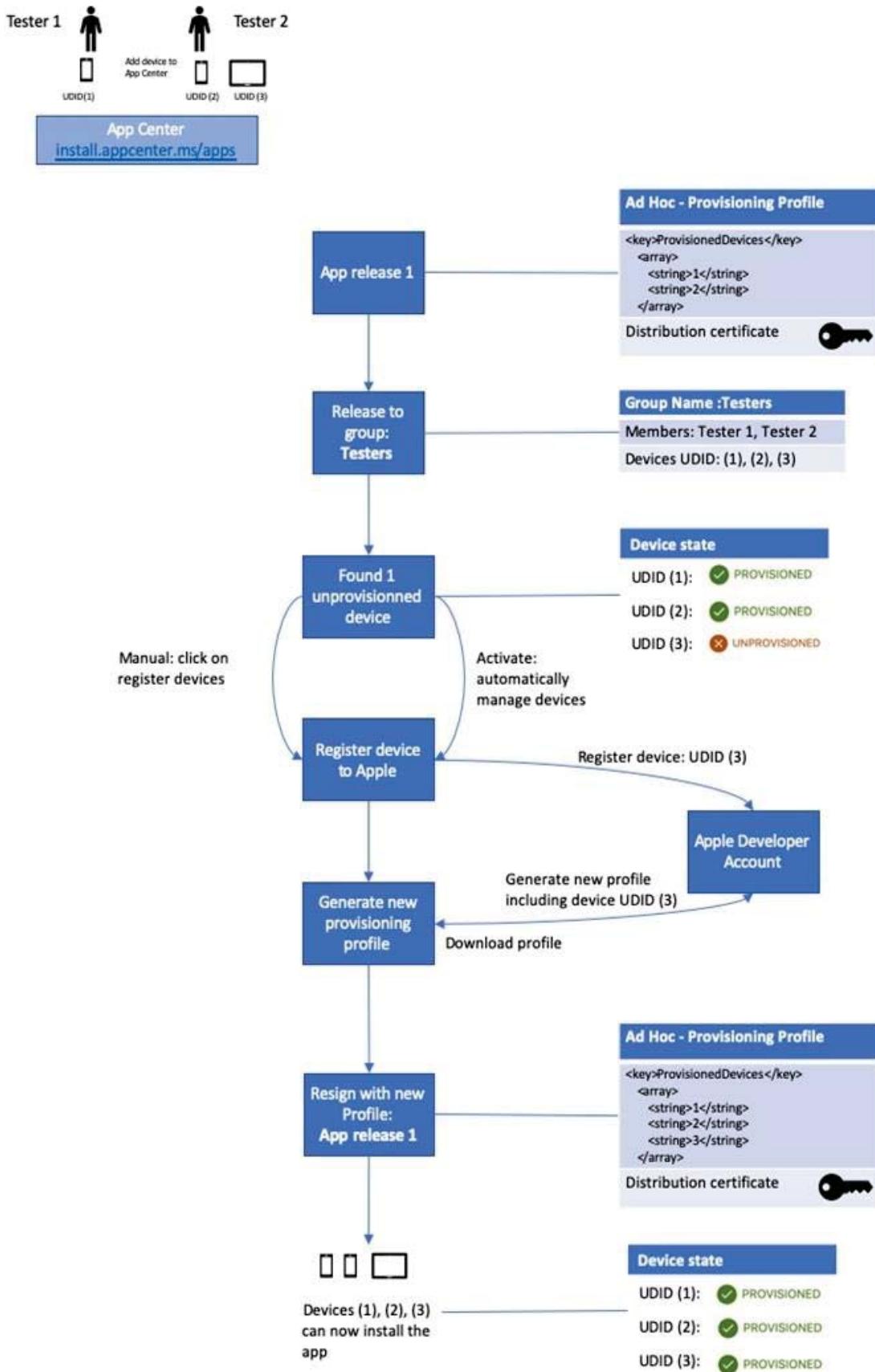
What should you do?

- 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.



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 164

Hotspot Question

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.

Answer Area

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:

Answer Area

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

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-cyrillic/azure/aks/azure-files-dynamic-pv><https://docs.microsoft.com/en-us/azure/aks/azure-disks-dynamic-pv>**QUESTION 165**

Hotspot Question

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.

Answer Area

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:

Answer Area

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 166

Drag and Drop Question

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.

Actions	Answer Area
Create a service account in the cluster.	
Create a service principal in Azure Active Directory (Azure AD).	
Add an Azure Function App for Container task to the deployment pipeline.	
Add a Helm package and deploy a task to the deployment pipeline.	
Add a Docker Compose task to the deployment pipeline.	
Configure RBAC roles in the cluster.	

Answer:

Actions	Answer Area
Create a service account in the cluster.	
Add an Azure Function App for Container task to the deployment pipeline.	
Configure RBAC roles in the cluster.	

Explanation:

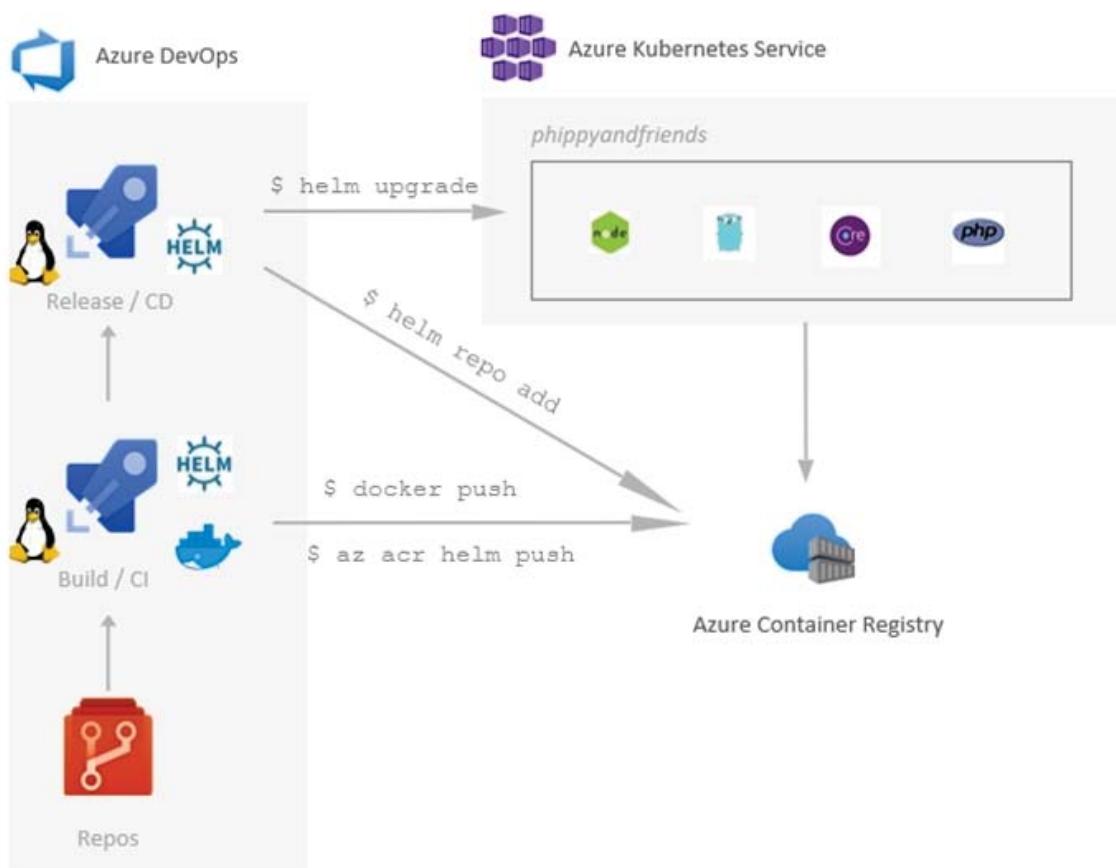
You can set up a CI/CD pipeline to deploy your apps on a Kubernetes cluster with Azure DevOps by leveraging a Linux agent, Docker, and Helm.

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 167

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

Explanation:

Instead reduce the code complexity.

Reference:

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

QUESTION 168

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 169

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

Explanation:

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

QUESTION 170

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

Incorrect Answers:

B, C: An epic represents a business initiative to be accomplished.

Epics, examples:

Increase customer engagement

Improve and simplify the user experience

Implement new architecture to improve performance

Engineer the application to support future growth

Support integration with external services

Support mobile apps

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 171

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 172

During a code review, you discover quality issues in a Java application.

You need to recommend a solution to detect quality issues including unused variables and empty catch blocks.

What should you recommend?

- A. In a Maven build task, select Run PMD.
- B. In an Xcode build task, select Use xcpretty from Advanced.
- C. In a Gulp build task, specify a custom condition expression.
- D. In a Grunt build task, select Enabled from Control Options.

Answer: A

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.

Incorrect Answers:

B: xcpretty is a fast and flexible formatter for xcbuild.

Reference:

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

QUESTION 173

Your company creates a new Azure DevOps team.

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://azuredevops.slabs.com/labs/azuredevops/agile/>

QUESTION 174

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. Bullseye Coverage
- B. JUnit
- C. JaCoCo
- D. NUnit

Answer: C

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.

Incorrect Answers:

A: Bullseye Coverage is used for C++ code, and not for Java.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-code-coverage-results>

QUESTION 175

SIMULATION

Your company plans to implement a new compliance strategy that will require all Azure web apps to be backed up every five hours.

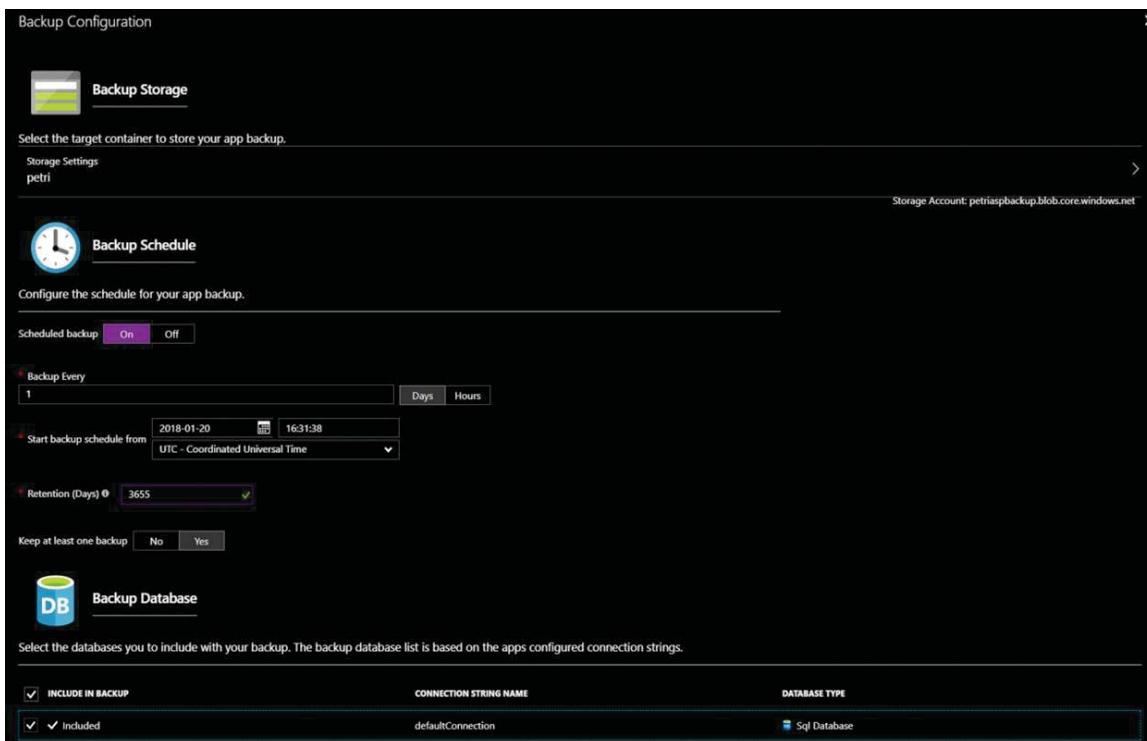
You need to back up an Azure web app named az400-11566895-main every five hours to an Azure Storage account in your resource group.

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

Answer:

With the storage account ready, you can configure backs up in the web app or App Service.

1. 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.
2. Select the storage account.
3. Click + to create a private container. You could name this container after the web app or App Service.
4. Select the container.
5. If you want to schedule backups, then set Scheduled Backup to On and configure a schedule: every five hours
6. Select your retention. Note that 0 means never delete backups.
7. Decide if at least one backup should always be retained.
8. Choose if any connected databases should be included in the web app backup.
9. Click Save to finalize the backup configuration.



Reference:

<https://petri.com/backing-azure-app-service>

QUESTION 176

SIMULATION

You need to configure a virtual machine named VM1 to securely access stored secrets in an Azure Key Vault named az400-11566895-kv.

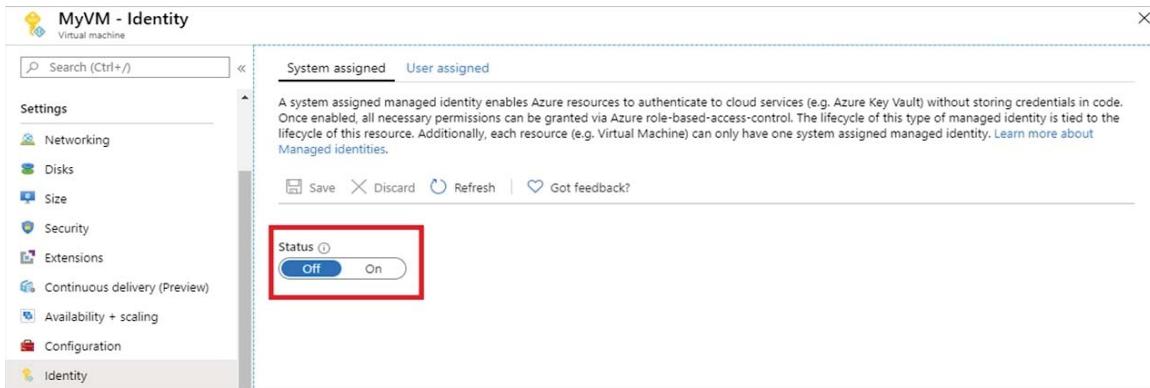
To complete this task, sign in to the Microsoft Azure portal.

Answer:

You can use a system-assigned managed identity for a Windows virtual machine (VM) to access Azure Key Vault.

10. Sign in to Azure portal

11. Locate virtual machine VM1.
12. Select Identity
13. 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 177

SIMULATION

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:

Enable Remote Debugging

Before we start a debugging session to our Azure Function app we need to enable the functionality.

14. Navigate in the Azure portal to your function app fa-11566895
15. Go to the “Application settings”
16. 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 178

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.

- 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.

C:

1. Select Add Access Policy.
2. Open Secret permissions and provide the app with Get and List permissions.
3. Select Select principal and select the registered app by name. Select the Select button.
4. Select OK.
5. Select Save.
6. Deploy the app.

References:

<https://docs.microsoft.com/en-us/aspnet/core/security/key-vault-configuration>

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 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 this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead, In Visual Designer you enable continuous integration (CI) by:

1. Select the Triggers tab.
2. Enable Continuous integration.

Reference:

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

QUESTION 180

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 181

SIMULATION

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:

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.

settings



A screenshot of the Azure portal Subscriptions page. At the top, there are tabs: SUBSCRIPTIONS, MANAGEMENT CERTIFICATES, ADMINISTRATORS, AFFINITY GROUPS, and USAGE. Below these tabs, there is a navigation bar with four items: SUBSCRIPTION, SUBSCRIPTION ID, ACCOUNT ADMINISTRATOR, and DIRECTORY. Under the DIRECTORY tab, the value "Windows Azure MSDN - Visual Studio Ultimate" is shown. To the right of this value is a red rectangular box highlighting the text "Joe Levy".

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.

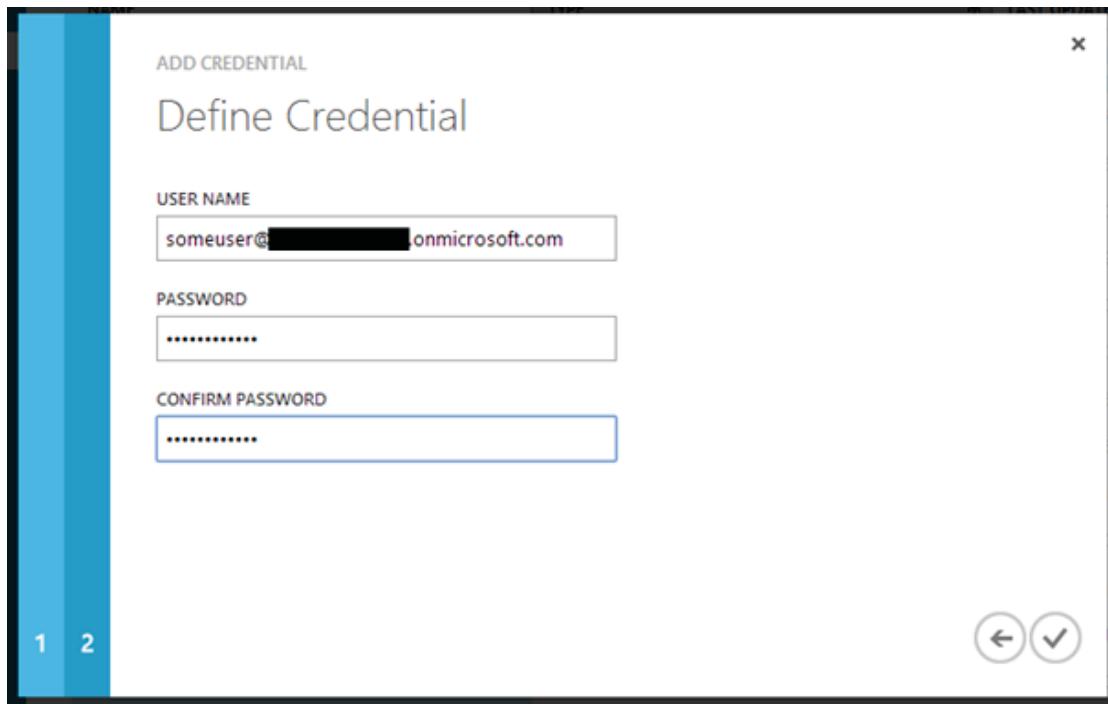
1. Click on Settings (bottom Azure tab under StorSimple)



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 182

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?

- 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

Explanation:

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 183

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: 

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://azuredavopslabs.com/labs/vstsextend/whitesource/>

QUESTION 184

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 185

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: 

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 186

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: 

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 187

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: 

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 188

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 189

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 190

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
- 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.

Incorrect Answers:

A: Use rebase to address the problem of updating your branch with the latest changes from the main branch. Rebase takes the changes made in the commits in your current branch and replays them on the history of another branch. The commit history of your current branch will be rewritten so that it starts from the most recent commit in the target branch of the rebase. Rebasing your changes in your feature branch off the latest changes in the main branch lets you test your changes on the most recent version in the main branch while keeping a clean Git history.

D: Share changes made in commits and branches using the push command. Push your branches to the remote repository. Git adds your commits to an existing branch on the remote or creates a new branch with the same commits as your local branch.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/pull-requests>

QUESTION 191

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: 
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 192**SIMULATION**

You manage a website that uses an Azure SQL Database named db1 in a resource group named RG1lod11566895.

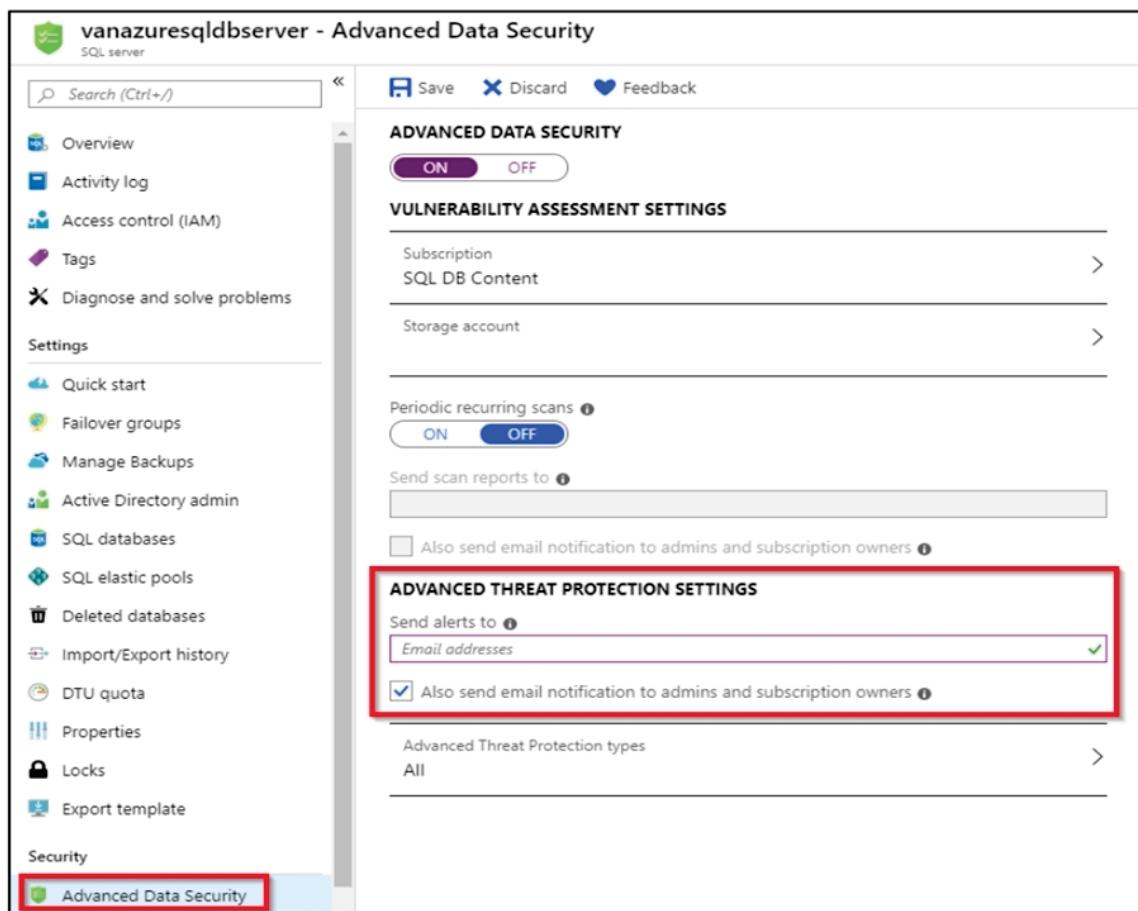
You need to modify the SQL database to protect against SQL injection.

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

Answer:

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:



The screenshot shows the Azure portal interface for managing a SQL server. The left sidebar lists various management options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Quick start, Failover groups, Manage Backups, Active Directory admin, SQL databases, SQL elastic pools, Deleted databases, Import/Export history, DTU quota, Properties, Locks, Export template, and Security. The 'Advanced Data Security' option is selected and highlighted with a red box. The main content area shows the 'ADVANCED DATA SECURITY' settings, with a toggle switch set to 'ON'. Below it are 'VULNERABILITY ASSESSMENT SETTINGS' and 'ADVANCED THREAT PROTECTION SETTINGS'. The 'ADVANCED THREAT PROTECTION SETTINGS' section is also highlighted with a red box. It includes fields for 'Send alerts to' (set to 'Email addresses') and a checked checkbox for 'Also send email notification to admins and subscription owners'.

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 193

SIMULATION

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

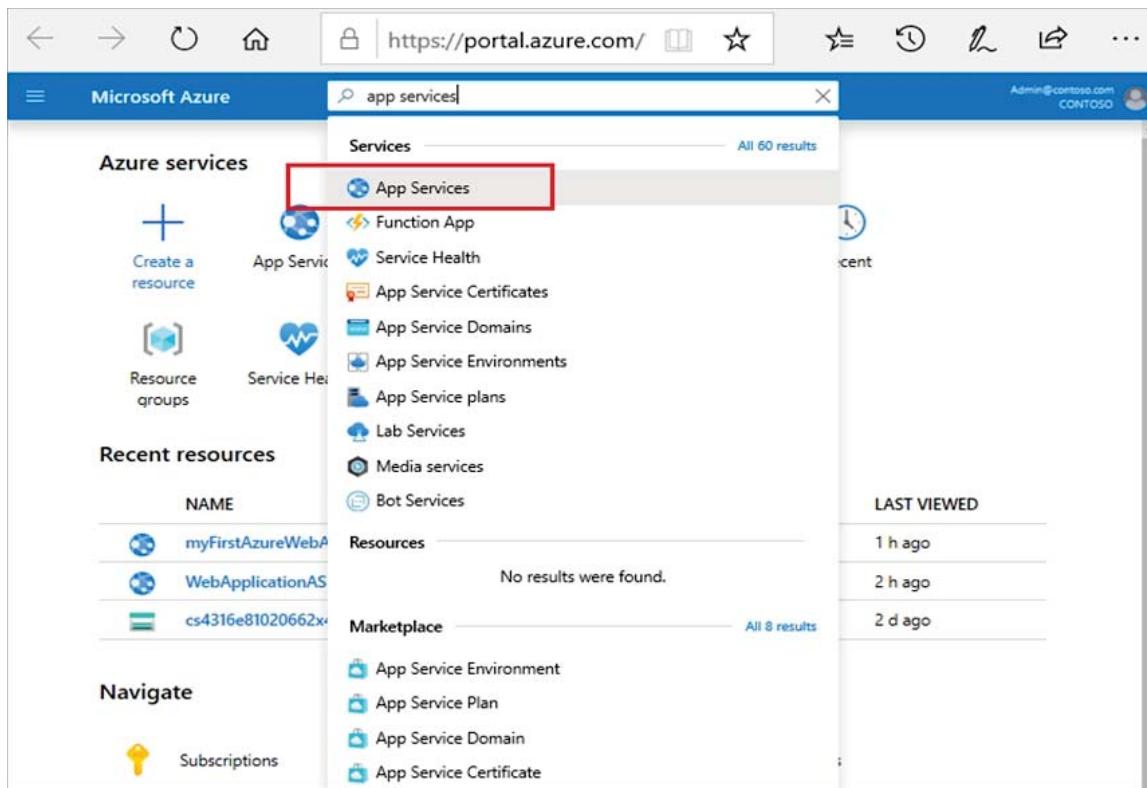
You need to configure a staging environment for az400-11566895-main.

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

Answer:

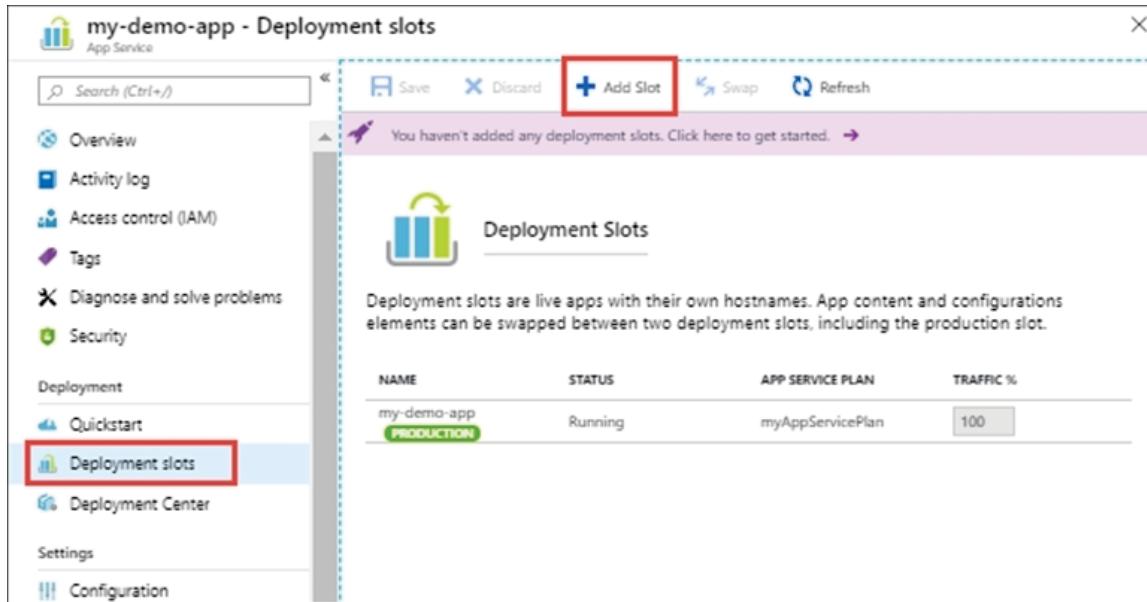
Add a slot

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



The screenshot shows the Microsoft Azure portal interface. The address bar at the top displays the URL <https://portal.azure.com/>. A search bar contains the text "app services". Below the search bar, the "Azure services" section is visible, featuring icons for "Create a resource", "Resource groups", "Recent resources", "Navigate", and "Subscriptions". On the right side, a search results panel titled "Services" shows "All 60 results". The "App Services" item is highlighted with a red box. Other listed items include Function App, Service Health, App Service Certificates, App Service Domains, App Service Environments, App Service plans, Lab Services, Media services, Bot Services, Resources (with a note: "No results were found."), Marketplace (with a note: "All 8 results"), and App Service Environment, App Service Plan, App Service Domain, and App Service Certificate.

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



The screenshot shows the "my-demo-app - Deployment slots" blade in the Azure portal. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Deployment (Quickstart, Deployment slots, Deployment Center), Settings, and Configuration. The "Deployment slots" link is highlighted with a red box. The main content area displays the "Deployment Slots" section with the following text: "Deployment slots are live apps with their own hostnames. App content and configurations elements can be swapped between two deployment slots, including the production slot." Below this is a table:

NAME	STATUS	APP SERVICE PLAN	TRAFFIC %
my-demo-app PRODUCTION	Running	myAppServicePlan	100

- 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.

Add a slot

Name
staging

Clone settings from:
Do not clone settings

Add **Close**

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

my-demo-app - Deployment slots

Deployment Slots

Deployment slots are live apps with their own hostnames. App content and configurations elements can be swapped between two deployment slots, including the production slot.

NAME	STATUS	APP SERVICE PLAN	TRAFFIC %
my-demo-app PRODUCTION	Running	myAppServicePlan	100
my-demo-app-staging	Running	myAppServicePlan	0

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

QUESTION 194

SIMULATION

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

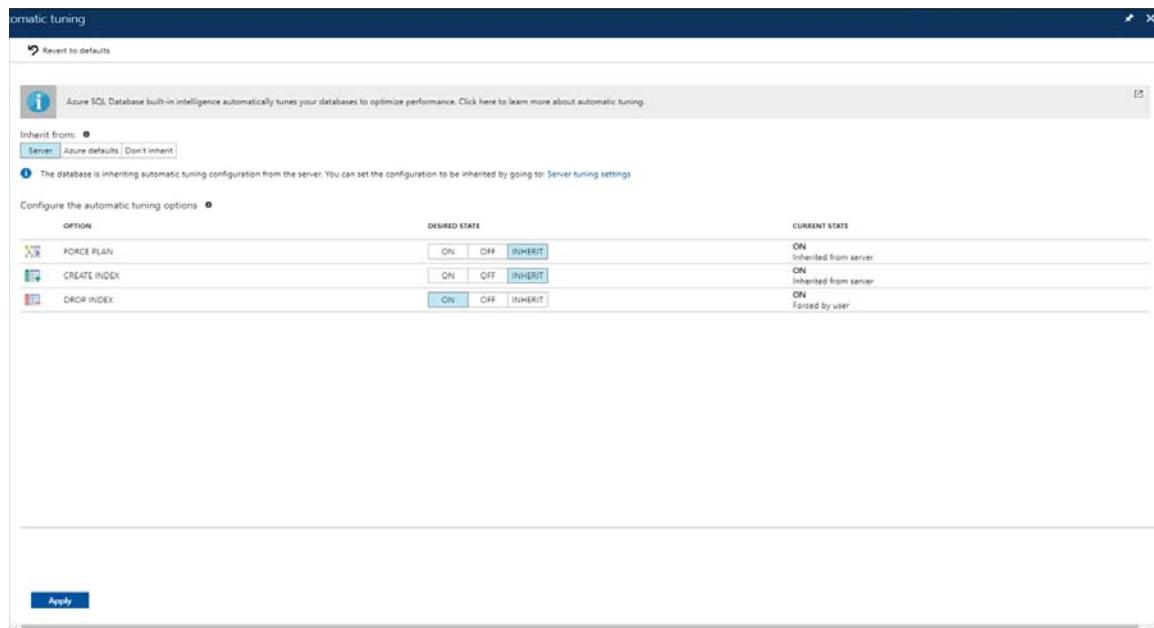
You need to ensure that queries to db1 are tuned by Azure over time. The solution must only

apply to db1.

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

Answer:

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 195

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 196**SIMULATION**

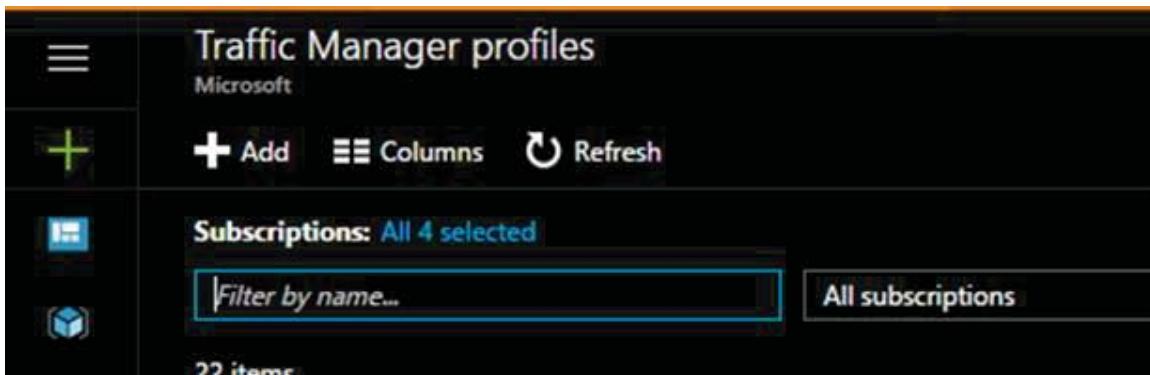
You plan to deploy a website that will be hosted in two Azure regions.

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:

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

Create Traffic Manager profi... □ X

* Name
samplegeoprofile .trafficmanager.net

Routing method
Geographic

* Subscription

* Resource group ⓘ
Create new Use existing
geoprofilerg

* Resource group location ⓘ
West US

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 197**SIMULATION**

You plan to add a new web farm that will be published by using an IP address of 10.0.0.5.

You need to allow traffic from the web farm to an Azure Database for MySQL server named az400-11566895-mysql.

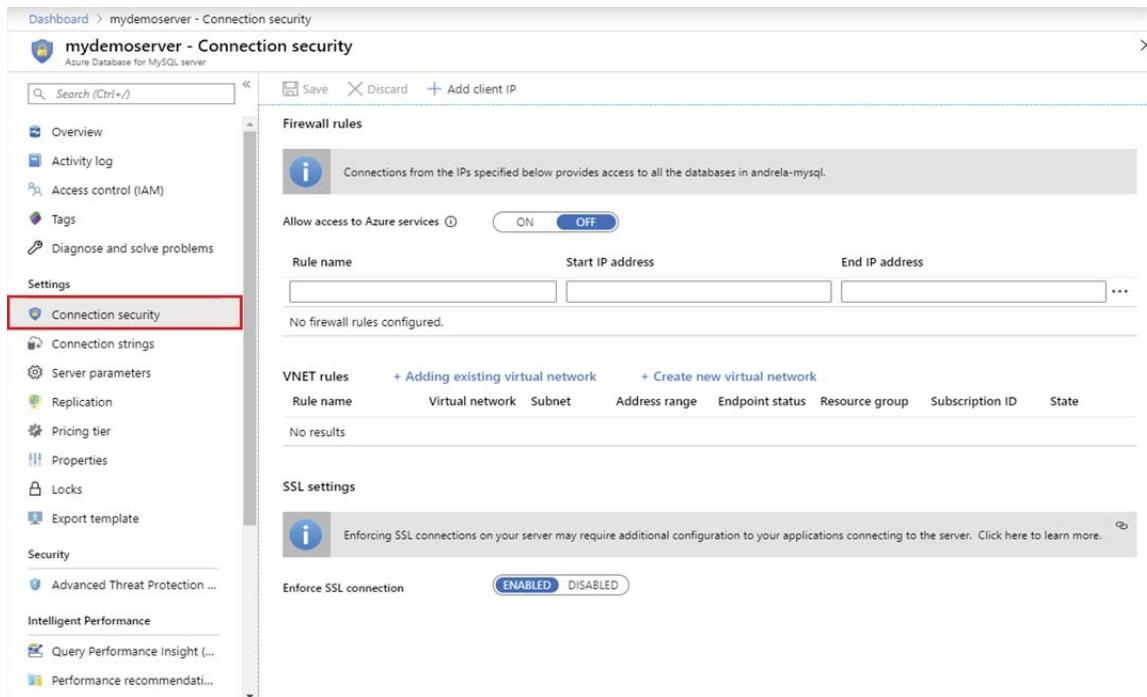
To complete this task, sign in to the Microsoft Azure portal.

Answer:

Server-level firewall rules can be used to manage access to an Azure Database for MySQL Server from a specified IP address or a range of IP addresses.

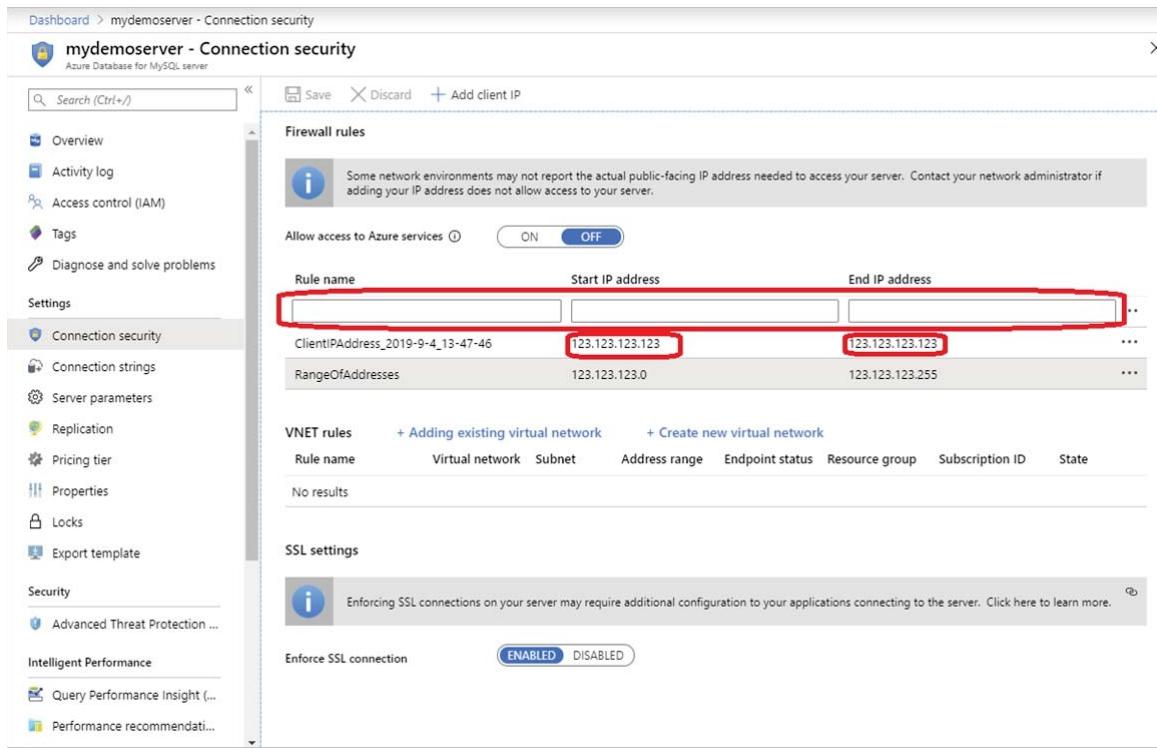
Create a server-level firewall rule in the Azure portal

1. On the MySQL server page, under Settings heading, click Connection Security to open the Connection Security page for the Azure Database for MySQL.



The screenshot shows the 'mydemoserver - Connection security' page in the Azure portal. The left sidebar has a 'Settings' section with 'Connection security' highlighted with a red box. The main content area is titled 'Firewall rules'. It contains an informational message: 'Connections from the IPs specified below provides access to all the databases in andrela-mysql.' Below this is a toggle switch for 'Allow access to Azure services' set to 'ON'. A table for 'Firewall rules' is shown with columns: Rule name, Start IP address, and End IP address. A note says 'No firewall rules configured.' Below this is a section for 'VNET rules' with buttons for '+ Adding existing virtual network' and '+ Create new virtual network'. A note says 'No results.' At the bottom is an 'SSL settings' section with an informational message about SSL enforcement, an 'Enforce SSL connection' toggle switch set to 'ENABLED', and a note about requiring additional application configuration.

2. In the firewall rules for the Azure Database for MySQL, you can specify a single IP address or a range of addresses. If you want to limit the rule to a single IP address, type the same address in the Start IP and End IP fields. Opening the firewall enables administrators, users, and application to access any database on the MySQL server to which they have valid credentials.



The screenshot shows the 'Connection security' settings for a MySQL server named 'mydemoserver'. The 'Firewall rules' section displays a table with two rows. The first row contains a rule named 'ClientIPAddress_2019-9-4_13-47-46' with 'Start IP address' set to '123.123.123.123' and 'End IP address' set to '123.123.123.255'. The second row is a header row for 'RangeOfAddresses' with values '123.123.123.0' and '123.123.123.255'. The 'Start IP address' and 'End IP address' columns are highlighted with red boxes.

3. Click Save on the toolbar to save this server-level firewall rule. Wait for the confirmation that the update to the firewall rules is successful.

Reference:

<https://docs.microsoft.com/en-us/azure/mysql/howto-manage-firewall-using-portal#create-a-server-level-firewall-rule-in-the-azure-portal>

QUESTION 198

You have a multi-tier application. The front end of the application is hosted in Azure App Service.

You need to identify the average load times of the application pages.

What should you use?

- A. Azure Application Insights
- B. the activity log of the App Service
- C. the diagnostics logs of the App Service
- D. Azure Advisor

Answer: A

Explanation:

Application Insights will tell you about any performance issues and exceptions, and help you find and diagnose the root causes.

Application Insights can monitor both Java and ASP.NET web applications and services, WCF services.

They can be hosted on-premises, on virtual machines, or as Microsoft Azure websites.

On the client side, Application Insights can take telemetry from web pages and a wide variety of devices including iOS, Android, and Windows Store apps.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/web-monitor-performance>**QUESTION 199****SIMULATION**

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:

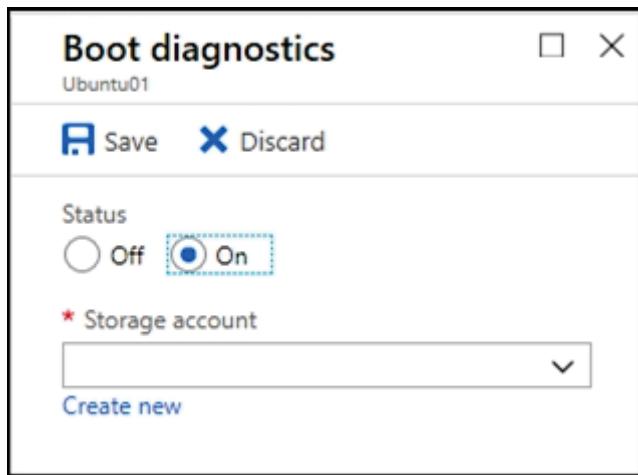
Step 1: To create a general-purpose v2 storage account in the Azure portal, follow these steps:

1. 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.
2. On the Storage Accounts window that appears, choose Add.
3. Select the subscription in which to create the storage account.
4. Under the Resource group field, select RG1lod11566895
5. Next, enter a name for your storage account named: az400lod11566895stor
6. 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 200
SIMULATION

You have a web app that connects to an Azure SQL Database named db1.

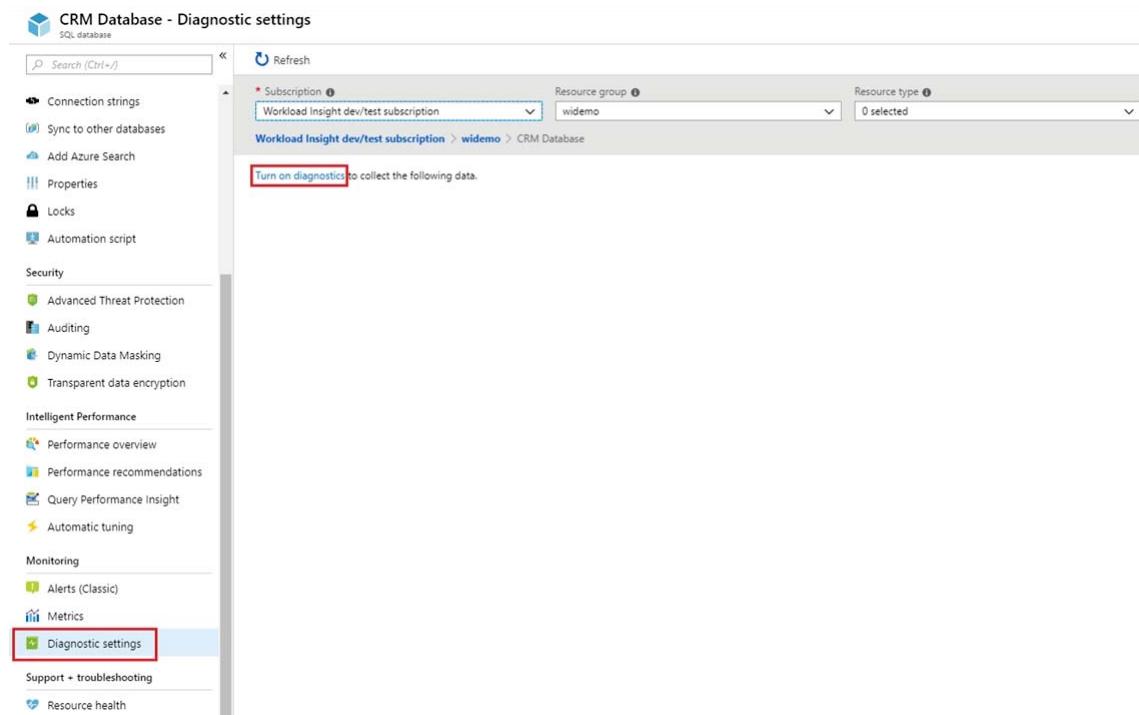
You need to configure db1 to send Query Store runtime statistics to Azure Log Analytics.

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

Answer:

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 X

*** Name**
 ✓

Archive to a storage account
 Stream to an event hub

Send to Log Analytics
Subscription
 ▼
Log Analytics Workspace
 ▼

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 201

Hotspot Question

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 type 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 Area

Branch lifetime:

	▼
Long-lived	
Short-lived	

Branch type:

	▼
Master	
Feature	
Integration	

Answer:

Answer Area

Branch lifetime:

	▼
Long-lived	
Short-lived	

Branch type:

	▼
Master	
Feature	
Integration	

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>

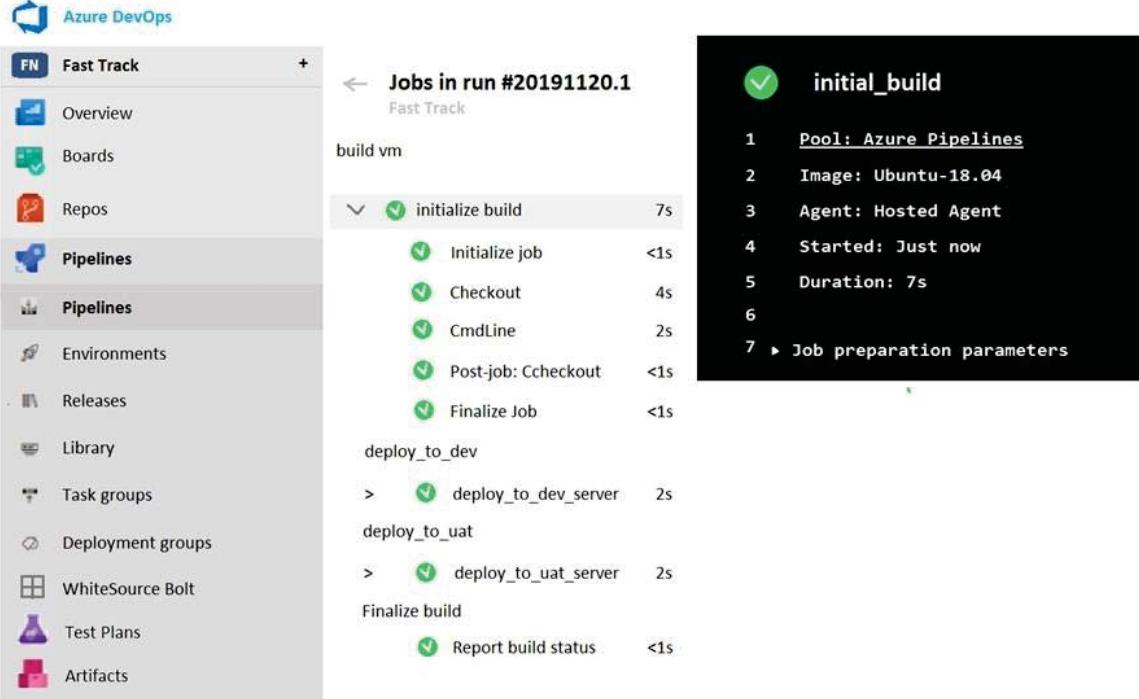
QUESTION 202

Hotspot Question

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.



The screenshot shows the Azure DevOps Pipelines interface. On the left, there's a sidebar with various options like Overview, Boards, Repos, Pipelines, Environments, Releases, Library, Task groups, Deployment groups, WhiteSource Bolt, Test Plans, and Artifacts. The 'Pipelines' option is selected. In the main area, it says 'Jobs in run #20191120.1' under 'Fast Track'. It lists several steps: 'build vm', 'initialize build' (which is expanded to show 'Initialize job', 'Checkout', 'CmdLine', 'Post-job: Ccheckout', and 'Finalize Job'), 'deploy_to_dev' (which is expanded to show 'deploy_to_dev_server'), 'deploy_to_uat' (which is expanded to show 'deploy_to_uat_server'), and 'Finalize build' (which is expanded to show 'Report build status'). A callout box highlights the first step, 'initial_build', with the following details:

initial_build

- 1 Pool: Azure Pipelines
- 2 Image: Ubuntu-18.04
- 3 Agent: Hosted Agent
- 4 Started: Just now
- 5 Duration: 7s
- 6
- 7 ▶ Job preparation parameters

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.

Answer Area

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:

Answer Area

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	

Explanation:

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

QUESTION 203

Drag and Drop Question

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:**Answer Area****Objects**

a cluster

a system-assigned managed identity

an application registration in contoso.com

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.

1. Sign in to the Azure portal.
2. In the search field at the top of the page, enter Azure Active Directory.
3. Click Enter.
4. In the Manage menu, select Users.
5. In the name field, search for your account.
6. In the Name column, select the link to your account.
7. In the Identity section, copy the Object ID.

Identity [edit](#)

Name
[REDACTED]

User name
[REDACTED]@hotmail.com

Object ID
[REDACTED] 

Step 3: a RBAC binding

Reference:

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

QUESTION 204

Hotspot Question

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.

Answer Area

Service connection type:	<input type="text"/>
	Azure Resource Manager
	Generic service
	Team Foundation Server / Azure Pipelines service connection
Authentication/authorization method for the connection:	<input type="text"/>
	Azure Active Directory OAuth 2.0
	Grant authorization
	Managed Service Identity Authentication

Answer:

Answer Area

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 205

Drag and Drop Question

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 Area	
Values	FROM <input type="text"/> <i>As build-env</i> COPY . /app/ WORKDIR /app RUN <input type="text"/> FROM <input type="text"/> COPY --from=build-env /app/out /app WORKDIR /app ENTRYPOINT ["dotnet", "MvcMovie.dll"]

Answer:

Answer Area		
Values	FROM Microsoft/dotnet:2.2-sdk	As build-env
dotnet publish -c Release -o out		
	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:

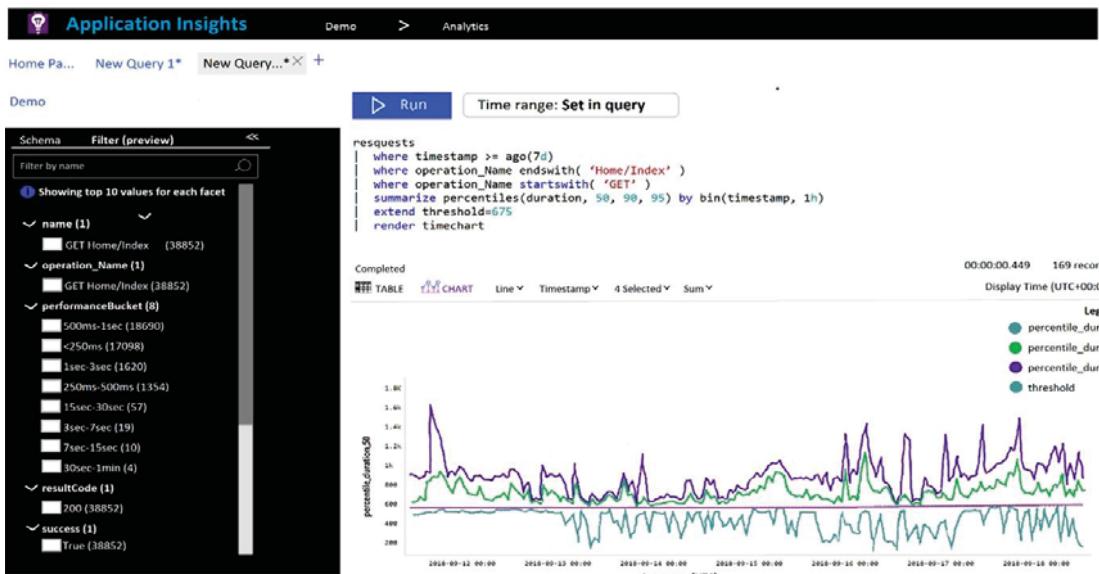
<https://docs.microsoft.com/de-DE/virtualization/windowscontainers/quick-start/building-sample-app>

QUESTION 206

Hotspot Question

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.

Answer Area

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:

Answer Area

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 207

Drag and Drop Question

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.

Answer Area**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:****Answer Area****Policy Types**

A status policy

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://azuredavolabs.com/labs/vstsextend/sonarcloud/>**QUESTION 208****Case Study 1 - Litware****Overview****Existing Environment**

Litware, Inc. is 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.NET web forms that use logic written in VB.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 live 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 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.

Customers report that bug reporting is overly complex.

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 existing retirement fund management system.

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.

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

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

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

Technical requirements

The company's investment planning applications suite must meet the following 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 releases must remain available for 30 days, except for production releases, which must be kept for 60 days.
- 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 HTTPS.

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

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 $vmaname  
-ConfigurationMode 'ApplyOnly'
```

Hotspot Question

How should you configure 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 Area

Required secrets:

Certificate
Personal access token
Shared Access Authorization token
Username and password

Storage location:

Azure Data Lake
Azure Key Vault
Azure Storage with HTTPS access
Azure Storage with HTTP access

Answer:

Answer Area

Required secrets:

Certificate
Personal access token
Shared Access Authorization token
Username and password

Storage location:

Azure Data Lake
Azure Key Vault
Azure Storage with HTTPS access
Azure Storage with HTTP access

Explanation:

Box 1: Shared Access Authorization token

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.

Box 2: Azure Storage with HTTPS access

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 application 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.

Reference:

<https://docs.microsoft.com/en-us/rest/api/storageservices/authorize-with-shared-key>

QUESTION 209

You use Azure Pipelines to manage project builds and deployments.

You plan to use Azure Pipelines for Microsoft Teams to notify the legal team when a new build is ready for release.

You need to configure the Organization Settings in Azure DevOps to support Azure Pipelines for Microsoft Teams.

What should you turn on?

- A. Third-party application access via OAuth

- B. Azure Active Directory Conditional Access Policy Validation
- C. Alternate authentication credentials
- D. SSH authentication

Answer: A

Explanation:

The Azure Pipelines app uses the OAuth authentication protocol, and requires Third-party application access via OAuth for the organization to be enabled. To enable this setting, navigate to Organization Settings > Security > Policies, and set the Third-party application access via OAuth for the organization setting to On.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams>

QUESTION 210

Your company implements an Agile development methodology.

You plan to implement retrospectives at the end of each sprint.

Which three questions should you include? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Who performed well?
- B. Who should have performed better?
- C. What could have gone better?
- D. What went well?
- E. What should we try next?

Answer: E



Explanation:

Sprint retrospective meetings

The sprint retrospective meeting typically occurs on the last day of the sprint, after the sprint review meeting. In this meeting, your team explores its execution of Scrum and what might need tweaking.

Based on discussions, your team might decide to change one or more processes to improve its own effectiveness, productivity, quality, and satisfaction. This meeting and the resulting improvements are critical to the agile principle of self-organization.

Look to address these areas during your team sprint retrospectives:

Issues that affected your team's general effectiveness, productivity, and quality.

Elements that impacted your team's overall satisfaction and project flow.

What happened to cause incomplete backlog items? What actions will the team take to prevent these issues in the future?

Reference:

<https://docs.microsoft.com/en-us/azure/devops/boards/sprints/best-practices-scrum>

QUESTION 211

Your company uses Azure Artifacts for package management.

You need to configure an upstream source in Azure Artifacts for Python packages.

Which repository type should you use as an upstream source?

- A. npmjs.org
- B. PyPI
- C. Maven Central
- D. third-party trusted Python

Answer: B

Explanation:

Get started with Python packages in Azure Artifacts

Create a feed

1. Select Artifacts (in the left navigation of your Azure DevOps project).
2. On the Artifacts page, select Create Feed.
3. In the Create new feed dialog box:
4. In the Name field, give the feed a name.

PyPI is the default repository name for twine, which is a tool for publishing Python packages.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/artifacts/quickstarts/python-packages>

QUESTION 212

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

You use a Git repository for applications source control.

You plan to create a new branch from an existing pull request. Later, you plan to merge the new branch and the target branch of the pull request.

You need to use a pull request action to create the new branch. The solution must ensure that the branch uses only a portion of the code in the pull request.

Which pull request action should you use?

- A. Set as default branch
- B. Approve with suggestions
- C. Cherry-pick
- D. Reactivate
- E. Revert

Answer: C

Explanation:

Cherry-pick a pull request

To copy changes made in a pull request to another branch in your repo, follow these steps:

1. In a completed pull request, select Cherry-pick, or for an active pull request, select Cherry-pick from the ... menu. Cherry-picking a pull request in this way creates a new branch with the copied changes.

Merge into a target branch in a second pull request.

2. In Target branch, enter the branch you want to merge the copied changes.
3. In Topic branch name, enter a new branch to contain the copied changes, then select Cherry-pick.
4. Select Create pull request to merge the topic branch into the target branch to complete the cherry-pick.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/pull-requests>

QUESTION 213

You have an Azure DevOps organization named Contoso that contains a project named Project1.

You provision an Azure key vault named Keyvault1.

You need to reference Keyvault1 secrets in a build pipeline of Project1.

What should you do first?

- A. Add a secure file to Project1.
- B. Create an XAML build service.
- C. Create a variable group in Project1.
- D. Configure the security policy of Contoso.

Answer: **Explanation:** 

Before this will work, the build needs permission to access the Azure Key Vault. This can be added in the Azure Portal.

Open the Access Policies in the Key Vault and add a new one. Choose the principle used in the DevOps build.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/release/azure-key-vault>

QUESTION 214

You are designing a build pipeline in Azure Pipelines.

The pipeline requires a self-hosted agent. The build pipeline will run once daily and will take 30 minutes to complete.

You need to recommend a compute type for the agent. The solution must minimize costs.

What should you recommend?

- A. an Azure Kubernetes Service (AKS) cluster
- B. Azure Container Instances
- C. an Azure virtual machine scale set
- D. Azure virtual machines

Answer: 

Explanation: If your pipelines are in Azure Pipelines, then you've got a convenient option to run your jobs using a Microsoft-hosted agent. With Microsoft-hosted agents, maintenance and upgrades are taken care of for you. Each time you run a pipeline, you get a fresh virtual machine. The virtual machine is discarded after one use. Microsoft-hosted agents can run jobs directly on the VM or in a container.

Note: You can try a Microsoft-hosted agent for no charge.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/hosted>

QUESTION 215

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 deployment.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation: Instead 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 216

Your company has an Azure DevOps project,

The source code for the project is stored in an on-premises repository and uses an on-premises build server.

You plan to use Azure DevOps to control the build process on the build server by using a self-hosted agent.

You need to implement the self-hosted agent.

You download and install the agent on the build server.

Which two actions should you perform next? Each correct answer presents part of the solution.

- A. From Azure, create a shared access signature (SAS).
- B. From the build server, create a certificate, and then upload the certificate to Azure Storage.
- C. From the build server, create a certificate, and then upload the certificate to Azure Key Vault.
- D. From DevOps, create a personal access token (PAT).
- E. From the build server, run config.cmd.

Answer: E

Explanation:

B: Make sure you install your self-signed ssl server certificate into the OS certificate store.

E: When you have a self-signed SSL certificate for your on-premises TFS server, make sure to configure the Git we shipped to allow that self-signed SSL certificate.

Enable git to use SChannel during configure with 2.129.0 or higher version agent Pass --gituseschannel during agent configuration

./config.cmd --gituseschannel

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/certificate>

QUESTION 217

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.

You are configuring a build pipeline in Azure Pipelines that will include a task named Task1. Task1 will authenticate by using an Azure AD service principal.

Which three values should you configure for Task1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the tenant ID
- B. the subscription ID
- C. the client secret
- D. the app ID
- E. the object ID

Answer: A,B,C

Explanation:

Create an Azure Resource Manager service connection with an existing service principal
AB: Enter the information about your service principal into the Azure subscription dialog

textboxes:

Tenant ID

Subscription ID

Subscription name

Service principal ID

Either the service principal client key or, if you have selected Certificate, enter the contents of both the certificate and private key sections of the *.pem file.

D: To deploy to a specific Azure resource, the task will need additional data about that resource.

If you're using the classic editor, select data you need. For example, the App service name.

If you're using YAML, then go to the resource in the Azure portal, and then copy the data into your code.

For example, to deploy a web app, you would copy the name of the App Service into the WebAppName value.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/library/connect-to-azure>

QUESTION 218

You need to execute inline testing of an Azure DevOps pipeline that uses a Docker deployment model. The solution must prevent the results from being published to the pipeline.

What should you use for the inline testing?

- A. a single stage Dockerfile

- B. an Azure Kubernetes Service (AKS) pod
- C. a multi-stage Dockerfile
- D. a Docker Compose file

Answer: 

Explanation:

Use Docker when running integration tests with Azure Pipelines.

Reference:

<https://crossprogramming.com/2019/12/27/use-docker-when-running-integration-tests-with-azure-pipelines.html>

QUESTION 219

You need to configure GitHub to use Azure Active Directory (Azure AD) for authentication.

What should you do first?

- A. Create a conditional access policy in Azure AD.
- B. Register GitHub in Azure AD.
- C. Create an Azure Active Directory B2C (Azure AD B2C) tenant.
- D. Modify the Security settings of the GitHub organization.

Answer: B

Explanation:

When you connect to a Git repository from your Git client for the first time, the credential manager prompts for credentials. Provide your Microsoft account or Azure AD credentials.

Note: Git Credential Managers simplify authentication with your Azure Repos Git repositories.

Credential managers let you use the same credentials that you use for the Azure DevOps Services web portal.

Credential managers support multi-factor authentication through Microsoft account or Azure Active Directory (Azure AD). Besides supporting multi-factor authentication with Azure Repos, credential managers also support two-factor authentication with GitHub repositories.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/set-up-credential-managers>

QUESTION 220

You have a project in Azure DevOps named Project1. Project1 contains a pipeline that builds a container image named Image1 and pushes Image1 to an Azure container registry named ACR1. Image1 uses a base image stored in Docker Hub.

You need to ensure that Image1 is updated automatically whenever the base image is updated.

What should you do?

- A. Enable the Azure Event Grid resource provider and subscribe to registry events.
- B. Add a Docker Hub service connection to Azure Pipelines.
- C. Create and run an Azure Container Registry task.
- D. Create a service hook in Project1.

Answer: C

Explanation:

ACR Tasks supports automated container image builds when a container's base image is updated, such as when you patch the OS or application framework in one of your base images.

Reference:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-tutorial-base-image-update>

QUESTION 221

You have a free tier of an Azure DevOps organization named Contoso. Contoso contains 10 private projects. Each project has multiple jobs with no dependencies.

You frequently run the jobs on five self-hosted agents but experience long build times and frequently queued builds.

You need to minimize the number of queued builds and the time it takes to run the builds.

What should you do?

- A. Configure the pipelines to use the Microsoft-hosted agents.
- B. Register additional self-hosted agents.
- C. Purchase self-hosted parallel jobs.
- D. Purchase Microsoft-hosted parallel jobs.

Answer: 

Explanation:

When the free tier is no longer sufficient, you can pay for additional capacity per parallel job.

Note: Microsoft-hosted CI/CD

If you want to run your jobs on machines that Microsoft manages, use Microsoft-hosted parallel jobs. Your jobs run on our pool of Microsoft-hosted agents.

We provide a free tier of service by default in every organization.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/licensing/concurrent-jobs>

QUESTION 222

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. Ansible
- B. Maven
- C. WhiteSource Bolt
- D. Helm

Answer: C

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.

Note: Blackduck would also be a good answer, but it is not an option here.

Reference:

<https://www.azuredevopslabs.com/labs/vstsextend/whitesource/>

QUESTION 223

Your company develops an application named App1 that is deployed in production.

As part of an application update, a new service is being added to App1. The new service requires access to an application named App2 that is currently in development.

You need to ensure that you can deploy the update to App1 before App2 becomes available. You must be able to enable the service in App1 once App2 is deployed.

What should you do?

- A. Implement a feature flag.
- B. Create a fork in the build.
- C. Create a branch in the build.
- D. Implement a branch policy.

Answer: A

Explanation:

Feature flags support a customer-first DevOps mindset, to enable (expose) and disable (hide) features in a solution, even before they are complete and ready for release.

Incorrect Answers:

C: Branch policies are an important part of the Git workflow and enable you to:

Isolate work in progress from the completed work in your master branch

Guarantee changes build before they get to master

Reference:

<https://docs.microsoft.com/en-us/azure/devops/migrate/phase-features-with-feature-flags>

QUESTION 224

You are designing the security validation strategy for a project in Azure DevOps.

You need to identify package dependencies that have known security issues and can be resolved by an update.

What should you use?

- A. Octopus Deploy
- B. Jenkins
- C. Gradle
- D. SonarQube

Answer: A

Explanation:

Incorrect Answers:

B: Jenkins is a popular open-source automation server used to set up continuous integration and delivery (CI/CD) for your software projects.

D: 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.

Reference:

<https://octopus.com/docs/packaging-applications>

QUESTION 225

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. Generate a new .p12 file for each device.
- B. Create an unsigned build.
- C. Register the devices on the Apple Developer portal.
- D. Create an active subscription in App Center Test.

Answer: C

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.

Reference:

<https://docs.microsoft.com/en-us/appcenter/distribution/groups>

QUESTION 226

Your company uses the following resources:

- Windows Server 2019 container images hosted in an Azure Container Registry.
- Azure virtual machines that run the latest version of Ubuntu
- An Azure Log Analytics workspace
- Azure Active Directory (Azure AD)
- An Azure key vault

For which two resources can you receive vulnerability assessments in Azure Security Center?
Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the Azure Log Analytics workspace
- B. the Azure key vault
- C. the Azure virtual machines that run the latest version of Ubuntu
- D. Azure Active Directory (Azure AD)

E. The Windows Server 2019 container images hosted in the Azure Container Registry.

Answer: D 

Explanation:
B: Azure Security Center includes Azure-native, advanced threat protection for Azure Key Vault, providing an additional layer of security intelligence.
C: When Security Center discovers a connected VM without a vulnerability assessment solution deployed, it provides the security recommendation "A vulnerability assessment solution should be enabled on your virtual machines".
Ubuntu supported versions: 12.04 LTS, 14.04 LTS, 15.x, 16.04 LTS, 18.04 LTS Reference: <https://docs.microsoft.com/en-us/azure/security-center/deploy-vulnerability-assessment-vm>

QUESTION 227

You have a private project in Azure DevOps.

You need to ensure that a project manager can create custom work item queries to report on the project's progress. The solution must use the principle of least privilege.

To which security group should you add the project manager?

- A. Reader
- B. Project Collection Administrators
- C. Project Administrators
- D. Contributor

Answer: D

Explanation:

Contributors have permissions to contribute fully to the project code base and work item tracking. The main permissions they don't have or those that manage or administer resources.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/organizations/security/permissions>

QUESTION 228

You use Azure Pipelines to manage build pipelines, GitHub to store source code, and Dependabot to manage dependencies.

You have an app named App1.

Dependabot detects a dependency in App1 that requires an update.

What should you do first to apply the update?

- A. Create a pull request.
- B. Approve the pull request.
- C. Create a branch.
- D. Perform a commit.

Answer: B

Explanation:

DependaBot is a useful tool to regularly check for dependency updates. By helping to keep your project up to date, DependaBot can reduce technical debt and immediately apply security vulnerabilities when patches are released. How does DependaBot work?

1. Dependabot regularly checks dependencies for updates
2. If an update is found, Dependabot creates a new branch with this upgrade and Pull Request for approval
3. You review the new Pull Request, ensure the tests passed, review the code, and decide if you can merge the change

Reference:

<https://samlearnsazure.blog/2019/12/20/github-using-dependabot/>

QUESTION 229

You are integrating Azure Pipelines and Microsoft Teams.

You install the Azure Pipelines app in Microsoft Teams.

You have an Azure DevOps organization named Contoso that contains a project name Project1.

You subscribe to Project1 in Microsoft Teams.

You need to ensure that you only receive events about failed builds in Microsoft Teams.

What should you do first?

- A. From Microsoft Teams, run @azure pipelines subscribe <https://dev.azure.com/Contoso/Project1>.
- B. From Azure Pipelines, add a Publish Build Artifacts task to Project1.
- C. From Microsoft Teams, run @azure pipelines subscriptions.
- D. From Azure Pipelines, enable continuous integration for Project1.

Answer: 

Explanation: 

To start monitoring all pipelines in a project, use the following command inside a channel:

@azure pipelines subscribe [project url]

The project URL can be to any page within your project (except URLs to pipelines).

For example:

@azure pipelines subscribe <https://dev.azure.com/myorg/myproject/>

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams>

QUESTION 230

You have an Azure DevOps organization named Contoso and an Azure subscription.

You use Azure DevOps to build and deploy a web app named App1. Azure Monitor is configured to generate an email notification in response to alerts generated whenever App1 generates a server-side error.

You need to receive notifications in Microsoft Teams whenever an Azure Monitor alert is generated.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create an Azure Monitor workbook.
- B. Create an Azure logic app that has an HTTP request trigger.
- C. Create an Azure logic app that has an Azure DevOps trigger.

- D. Modify an action group in Azure Monitor.
- E. Modify the Diagnostics settings in Azure Monitor.

Answer: CD
Explanation: 

<https://dirteam.com/dave/2019/05/14/getting-azure-devops-tasks-in-to-do-with-flow/>

QUESTION 231

You have a Microsoft ASP.NET Core web app in Azure that is accessed worldwide.

You need to run a URL ping test once every five minutes and create an alert when the web app is unavailable from specific Azure regions. The solution must minimize development time.

What should you do?

- A. Create an Azure Monitor Availability metric and alert.
- B. Create an Azure Application Insights availability test and alert.
- C. Write an Azure function and deploy the function to the specific regions.
- D. Create an Azure Service Health alert for the specific regions.

Answer: B

Explanation:

There are three types of Application Insights availability tests:

URL ping test: a simple test that you can create in the Azure portal.

Multi-step web test

Custom Track Availability Tests

Note: After you've deployed your web app/website, you can set up recurring tests to monitor availability and responsiveness. Azure Application Insights sends web requests to your application at regular intervals from points around the world. It can alert you if your application isn't responding, or if it responds too slowly.

You can set up availability tests for any HTTP or HTTPS endpoint that is accessible from the public internet. You don't have to make any changes to the website you're testing. In fact, it doesn't even have to be a site you own. You can test the availability of a REST API that your service depends on.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability#create-a-url-ping-test>

QUESTION 232

You are designing a strategy to monitor the baseline metrics of Azure virtual machines that run Windows Server.

You need to collect detailed data about the processes running in the guest operating system.

Which two agents should you deploy? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the Telegraf agent
- B. the Azure Log Analytics agent

- C. the Azure Network Watcher Agent for Windows
- D. the Dependency agent

Answer: BD

Explanation:

The following table provide a quick comparison of the Azure Monitor agents for Windows.

	Azure Monitor agent (preview)	Diagnostics extension (WAD)	Log Analytics agent	Dependency agent
Environments supported	Azure	Azure Other cloud On-premises	Azure Other cloud On-premises	Azure Other cloud On-premises
Agent requirements	None	None	None	Requires Log Analytics agent
Data collected	Event Logs Performance File based logs IIS logs .NET app logs Crash dumps Agent diagnostics logs	Event Logs ETW events Performance File based logs IIS logs Insights and solutions Other services	Event Logs Performance File based logs IIS logs Insights and solutions Other services	Process dependencies Network connection metrics
Data sent to	Azure Monitor Logs Azure Monitor Metrics	Azure Storage Azure Monitor Metrics Event Hub	Azure Monitor Logs Azure Monitor Metrics	Azure Monitor Logs (through Log Analytics agent)

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview>

QUESTION 233

You configure an Azure Application Insights availability test.

You need to notify the customer services department at your company by email when availability is degraded.

You create an Azure logic app that will handle the email and follow up actions.

Which type of trigger should you use to invoke the logic app?

- A. an HTTPWebhook trigger
- B. an HTTP trigger
- C. a Request trigger
- D. an ApiConnection trigger

Answer: 
Explanation:

You can use webhooks to route an Azure alert notification to other systems for post-processing or custom actions. You can use a webhook on an alert to route it to services that send SMS messages, to log bugs, to notify a team via chat or messaging services, or for various other actions.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-webhooks>

QUESTION 234

You have an Azure DevOps organization named Contoso and an Azure subscription.

You use Azure DevOps to build a containerized app named App1 and deploy App1 to an Azure container instance named ACI1.

You need to restart ACI1 when App1 stops responding.

What should you do?

- A. Add a liveness probe to the YAML configuration of App1.
- B. Add a readiness probe to the YAML configuration of App1.
- C. Use Connection Monitor in Azure Network Watcher.
- D. Use IP flow verify in Azure Network Watcher.

Answer: 
Explanation:

For containerized applications that serve traffic, you might want to verify that your container is ready to handle incoming requests. Azure Container Instances supports readiness probes to include configurations so that your container can't be accessed under certain conditions. The readiness probe behaves like a Kubernetes readiness probe. For example, a container app might need to load a large data set during startup, and you don't want it to receive requests during this time.

YAML is used to setup a liveness probe.

Reference:

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-readiness-probe>

QUESTION 235

Drag and Drop Question

You manage the Git repository for a large enterprise application.

During the development of the application, you use a file named Config.json.

You need to prevent Config.json from being committed to the source control whenever changes to the application are committed.

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	Answer Area
Delete and recreate the repository.	
Run the <code>git reflog expire</code> command.	(Up)
Run the <code>git add .gitignore</code> command.	(Down)
Add Config.json to the <code>.gitignore</code> file.	(Up)
Run the <code>git commit</code> command.	(Down)

Answer:

Actions	Answer Area	
	Delete and recreate the repository.	
Run the <code>git reflog expire</code> command.	(Up)	
	Add Config.json to the <code>.gitignore</code> file.	
	Run the <code>git add .gitignore</code> command.	(Up)
Run the <code>git commit</code> command.	(Down)	

Explanation:



Step 1: Delete and recreate the repository.

Step 2: Add Config.json to the `.gitignore` file

Each line in the `.gitignore` excludes a file or set of files that match a pattern.

Example:

ignore a single file

Config.json

Step 3: Run the `git add .gitignore` command

At the initial commit we want basically move from Untracked to Staged, for staging we have to indicate which file we want to move or specify a pattern, as example:

Reference:

<http://hermit.no/how-to-find-the-best-gitignore-for-visual-studio-and-azure-devops/>

<https://geohernandez.net/how-to-add-an-existing-repository-into-azure-devops-repo-with-git/>

QUESTION 236

Drag and Drop Question

You are deploying a new application that uses Azure virtual machines.

You plan to use the Desired State Configuration (DSC) extension on the virtual machines.

You need to ensure that the virtual machines always have the same Windows feature installed.

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	Answer Area
Configure the DSC extension on the virtual machines.	
Create a YAML configuration file.	
Load the file to Azure Blob storage.	
Configure the Custom Script Extension on the virtual machines.	
Load the file to Azure Files.	
Create a PowerShell configuration file.	

Answer:

Actions

Configure the DSC extension on the virtual machines.

Create a YAML configuration file.

Answer Area

Create a PowerShell configuration file.

Load the file to Azure Blob storage.



Configure the Custom Script Extension on the virtual machines.

Load the file to Azure Files.

Explanation:

Step 1: Create a PowerShell configuration file

You create a simple PowerShell DSC configuration file.

Step 2: Load the file to Azure Blob storage

Package and publish the module to a publically accessible blob container URL

Step 3: Configure the Custom Script Extension on the virtual machines. The Custom Script Extension downloads and executes scripts on Azure virtual machines.

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started>

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/custom-script-windows>

QUESTION 237

Drag and Drop Question

You need to deploy Internet Information Services (IIS) to an Azure virtual machine that runs Windows Server 2019.

How should you complete the Desired State Configuration (DSC) configuration script? To answer, drag the appropriate values to the correct locations. Each value 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.

Values

Configuration
DependsOn
File
IncludeAllSubFeature
WindowsFeature

Answer Area

```
MyDsc {
    Node 'Server1' {
        MyConfigDetail {
            Ensure = 'Present'
            Name = 'Web-Server'
        }
    }
}
MyDsc
```

Answer:
Values

Configuration
DependsOn
File
IncludeAllSubFeature

Answer Area

```
MyDsc {
    Node 'Server1' {
        WindowsFeature MyConfigDetail {
            Ensure = 'Present'
            Name = 'Web-Server'
        }
    }
}
MyDsc
```

Explanation:

Box 1: Configuration

The following example shows a simple example of a configuration.

```
configuration IISInstall
{
    node "localhost"
    {
        WindowsFeature IIS
        {
            Ensure = "Present"
        }
    }
}
```

```
Name = "Web-Server"
}
}
```

}

Box 2: WindowsFeature

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview>

QUESTION 238

Drag and Drop Question

You are building an application that has the following assets:

- Source code
- Logs from automated tests and builds
- Large and frequently updated binary assets
- A common library used by multiple applications

Where should you store each asset? To answer, drag the appropriate Azure services to the correct assets. Each service may be used once. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Azure Services Answer Area

Azure Artifacts

Source code:

Azure Pipelines

A common library used by multiple applications:

Azure Repos

Logs from automated tests and builds:

Azure Storage

Large and frequently updated binary assets:

Azure Test Plans

Answer:



Azure Services

Answer Area

Source code:

Azure Repos

A common library used by multiple applications:

Azure Artifacts

Logs from automated tests and builds:

Azure Pipelines

Large and frequently updated binary assets:

Azure Storage

Azure Test Plans

Explanation:

Box 1: Azure Repos

Box 2: Azure Artifacts

Use Azure Artifacts to create, host, and share packages with your team.

Box 3: Azure Pipelines

In the pipeline view you can see all the stages and associated tests. The view provides a summary of the test results

Box 4: Azure Storage

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/get-started/what-is-repos>

<https://azure.microsoft.com/en-us/services/devops/artifacts/>

<https://docs.microsoft.com/en-us/azure/devops/pipelines/test/review-continuous-test-results-after-build>

QUESTION 239

Drag and Drop Question

You have several Azure virtual machines that run Windows Server 2019.

You need to identify the distinct event IDs of each virtual machine as shown in the following table.

Name	Event ID
VM1	[704, 701, 1501, 1500, 1085]
VM2	[326, 105, 302, 301, 300, 102]
...	...

How should you complete the Azure Monitor query? To answer, drag the appropriate values to the correct locations. Each value 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.

Values	Answer Area
count()	Event
makelist(EventID)	where TimeGenerated > ago(12h)
makeset(EventID)	order by TimeGenerated desc
mv-expand	[] [] by Computer
project	
render	
summarize	

Answer:

Values	Answer Area
count()	Event
	where TimeGenerated > ago(12h)
makelist(EventID)	order by TimeGenerated desc
mv-expand	[summarise] [makelist(EventID)] by Computer
project	
render	



Explanation:

You can use makelist to pivot data by the order of values in a particular column. For example, you may want to explore the most common order events take place on your machines. You can essentially pivot the data by the order of EventIDs on each machine.

Example:

Event
 | where TimeGenerated > ago(12h)
 | order by TimeGenerated desc
 | summarize makelist(EventID) by Computer

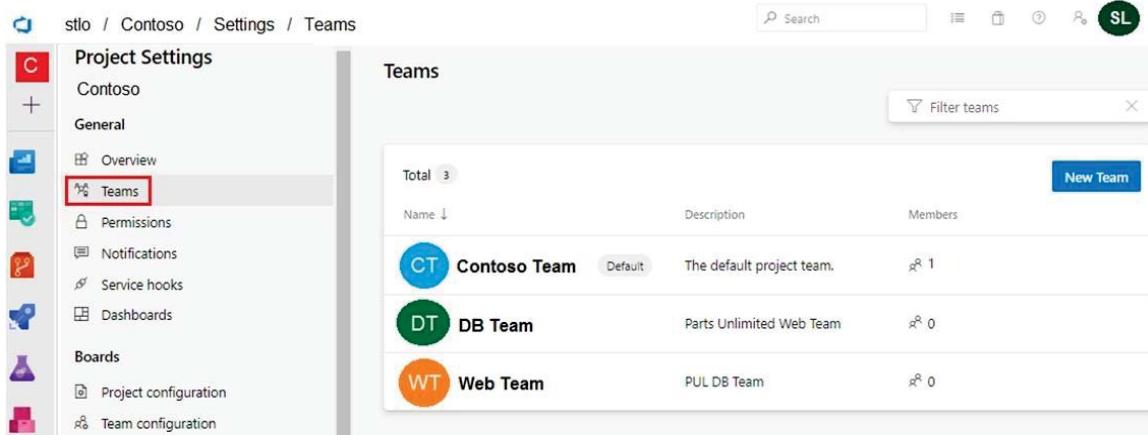
Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/advanced-aggregations>

QUESTION 240

Hotspot Question

You have a project in Azure DevOps that has three teams as shown in the Teams exhibit. (Click the Teams tab.)

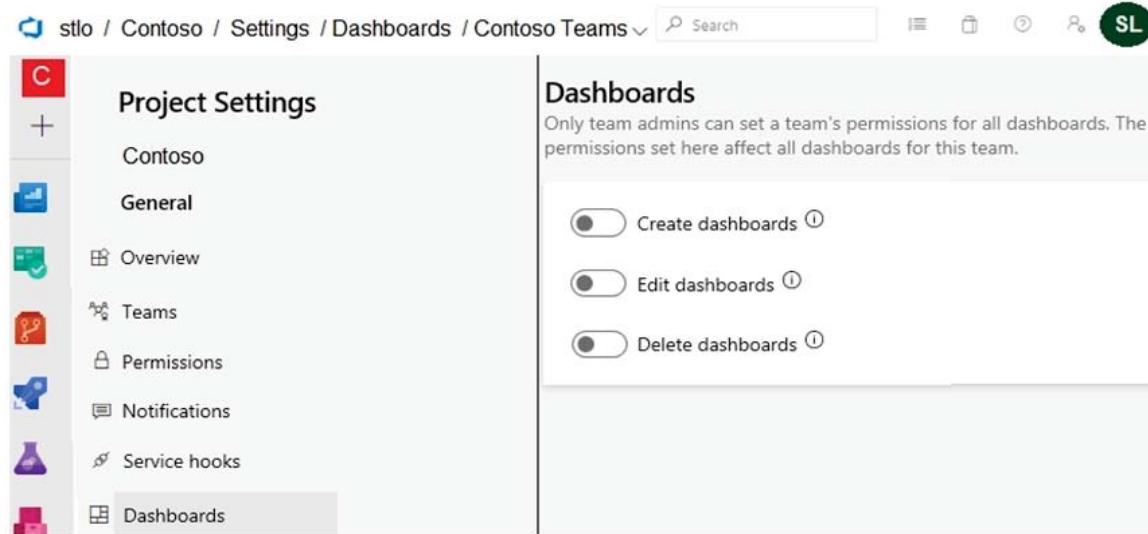


The screenshot shows the 'Teams' section of the Azure DevOps interface. On the left, a sidebar menu includes 'Project Settings' (selected), 'General', 'Overview', 'Teams' (highlighted with a red box), 'Permissions', 'Notifications', 'Service hooks', 'Dashboards', 'Boards', 'Project configuration', and 'Team configuration'. The main area displays a table titled 'Teams' with the following data:

Name	Description	Members
Contoso Team	The default project team.	1
DB Team	Parts Unlimited Web Team	0
Web Team	PUL DB Team	0

You create a new dashboard named Dash1.

You configure the dashboard permissions for the Control project as shown in the Permissions exhibit. (Click the Permissions tab.)



The screenshot shows the 'Permissions' section of the Azure DevOps interface. On the left, a sidebar menu includes 'Project Settings' (selected), 'General', 'Overview', 'Teams', 'Permissions' (highlighted with a red box), 'Notifications', 'Service hooks', and 'Dashboards'. The main area is titled 'Dashboards' and contains the following text: 'Only team admins can set a team's permissions for all dashboards. The permissions set here affect all dashboards for this team.' Below this are three toggle switches:

- Create dashboards
- Edit dashboards
- Delete dashboards

All other permissions have the default values set.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Web Team can delete Dash1.	<input type="radio"/>	<input type="radio"/>
Contoso Team can view Dash1.	<input type="radio"/>	<input type="radio"/>
Project administrators can create new dashboards.	<input checked="" type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Web Team can delete Dash1.	<input type="radio"/>	<input checked="" type="radio"/>
Contoso Team can view Dash1.	<input checked="" type="radio"/>	<input type="radio"/>
Project administrators can create new dashboards.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

<https://docs.microsoft.com/en-us/azure/devops/report/dashboards/charts-dashboard-permissions-access>

QUESTION 241

You have an existing project in Azure DevOps.

You plan to integrate GitHub as the repository for the project.

You need to ensure that Azure Pipelines runs under the Azure Pipelines identity.

Which authentication mechanism should you use?

- A. personal access token (PAT)
- B. GitHub App
- C. Azure Active Directory (Azure AD)
- D. OAuth

Answer: B

Explanation:

GitHub App uses the Azure Pipelines identity.

Incorrect Answers:

A: Personal access token and OAuth use your personal GitHub identity.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/github>

QUESTION 242

You plan to provision a self-hosted Linux agent.

Which authentication mechanism should you use to register the self-hosted agent?

- A. personal access token (PAT)
- B. SSH key
- C. Alternate credentials
- D. certificate

Answer: A**Explanation:**

Note: PAT Supported only on Azure Pipelines and TFS 2017 and newer. After you choose PAT, paste the PAT token you created into the command prompt window. Use a personal access token (PAT) if your Azure DevOps Server or TFS instance and the agent machine are not in a trusted domain. PAT authentication is handled by your Azure DevOps Server or TFS instance instead of the domain controller.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-linux>

QUESTION 243

You are building a Microsoft ASP.NET application that requires authentication.

You need to authenticate users by using Azure Active Directory (Azure AD).

What should you do first?

- A. Assign an enterprise application to users and groups
- B. Create an app registration in Azure AD
- C. Configure the application to use a SAML endpoint
- D. Create a new OAuth token from the application
- E. Create a membership database in an Azure SQL database

Answer: B**Explanation:**

Register your application to use Azure Active Directory. Registering the application means that your developers can use Azure AD to authenticate users and request access to user resources such as email, calendar, and documents.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/developer-guidance-for-integrating-applications>

QUESTION 244

You plan to create in Azure DevOps. Multiple developers will work on the project. The developers

will work offline frequently and will require access to the full project history while they are offline.

Which version control solution should you use?

- A. Team Foundation Version Control
- B. Git
- C. TortoiseSVN
- D. Subversion

Answer: B

Explanation:

Git history: File history is replicated on the client dev machine and can be viewed even when not connected to the server. You can view history in Visual Studio and on the web portal.

Note: Azure Repos supports two types of version control: Git and Team Foundation Version Control (TFVC).

Incorrect Answers:

A: Team Foundation Version Control: File history is not replicated on the client dev machine and so can be viewed only when you're connected to the server.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/comparison-git-tfvc>

QUESTION 245

You have the following Azure policy.

```
if: {
  allOf: [
    {
      "field": "type",
      "equals": "Microsoft.Storage/storageAccounts"
    },
    {
      "field": "Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly",
      "notEquals": "true"
    }
  ],
  then: {
    effect: "deny"
  }
}
```

You assign the policy to the Tenant root group.

What is the effect of the policy?

- A. prevents all http traffic to existing Azure Storage accounts
- B. ensures that all traffic to new Azure Storage accounts is encrypted
- C. prevents HTTPS traffic to new Azure Storage accounts when the accounts are accessed over the Internet
- D. ensures that all data for new Azure Storage accounts is encrypted at rest

Answer: B

Explanation:

Denies non HTTPS traffic.

QUESTION 246

You have a build pipeline in Azure Pipelines that uses different jobs to compile an application for 10 different architectures.

The build pipeline takes approximately one day to complete.

You need to reduce the time it takes to execute the build pipeline.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Move to a blue/green deployment pattern
- B. Create a deployment group
- C. Increase the number of parallel jobs
- D. Reduce the size of the repository
- E. Create an agent pool

Answer: CE

Explanation:

Question: I need more hosted build resources. What can I do?

Answer: The Azure Pipelines pool provides all Azure DevOps organizations with cloud-hosted build agents and free build minutes each month. If you need more Microsoft-hosted build resources, or need to run more jobs in parallel, then you can either:

Host your own agents on infrastructure that you manage.

Buy additional parallel jobs.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues>

QUESTION 247

You are creating a build pipeline in Azure Pipelines.

You define several tests that might fail due to third-party applications.

You need to ensure that the build pipeline completes successfully if the third-party applications are unavailable.

What should you do?

- A. Configure the build pipeline to use parallel jobs
- B. Configure flaky tests
- C. Increase the test pass percentage
- D. Add the Requirements quality widget to your dashboard

Answer: D

Explanation:

Requirements traceability is the ability to relate and document two or more phases of a development process, which can then be traced both forward or backward from its origin. Requirements traceability help teams to get insights into indicators such as quality of requirements or readiness to ship the requirement.

A fundamental aspect of requirements traceability is association of the requirements to test cases, bugs and code changes.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/test/requirements-traceability>

QUESTION 248

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. Gradle
- B. Chef
- C. Grunt
- D. Gulp

Answer: A

Explanation:

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.

Reference:

<https://docs3.sonarqube.org/latest/analysis/scan/sonarscanner-for-azure-devops/>

QUESTION 249

You are designing a configuration management solution to support five apps hosted on Azure App Service. Each app is available in the following three environments: development, test, and production.

You need to recommend a configuration management solution that meets the following requirements:

- Supports feature flags
- Tracks configuration changes from the past 30 days
- Stores hierarchically structured configuration values
- Controls access to the configurations by using role-based access control (RBAC) permission
- Stores shared values as key/value pairs that can be used by all the apps

Which Azure service should you recommend as the configuration management solution?

- A. Azure Cosmos DB
- B. Azure App Service
- C. Azure App Configuration
- D. Azure Key Vault

Answer: C

Explanation:

The Feature Manager in the Azure portal for App Configuration provides a UI for creating and managing the feature flags that you use in your applications.

App Configuration offers the following benefits:

- A fully managed service that can be set up in minutes
- Flexible key representations and mappings
- Tagging with labels
- Point-in-time replay of settings
- Dedicated UI for feature flag management
- Comparison of two sets of configurations on custom-defined dimensions
- Enhanced security through Azure-managed identities
- Encryption of sensitive information at rest and in transit
- Native integration with popular frameworks

App Configuration complements Azure Key Vault, which is used to store application secrets.

Reference:
<https://docs.microsoft.com/en-us/azure/azure-app-configuration/overview>

QUESTION 250

You have a containerized solution that runs in Azure Container Instances. The solution contains a frontend container named App1 and a backend container named DB1. DB1 loads a large amount of data during startup.

You need to verify that DB1 can handle incoming requests before users can submit requests to App1.

What should you configure?

- A. a liveness probe
- B. a performance log
- C. a readiness probe
- D. an Azure Load Balancer health probe

Answer: C

Explanation:

For containerized applications that serve traffic, you might want to verify that your container is ready to handle incoming requests. Azure Container Instances supports readiness probes to include configurations so that your container can't be accessed under certain conditions.

Incorrect Answers:

A: Containerized applications may run for extended periods of time, resulting in broken states that may need to be repaired by restarting the container. Azure Container Instances supports liveness probes so that you can configure your containers within your container group to restart if critical functionality is not working.

Reference:

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-readiness-probe>

QUESTION 251

You have an Azure DevOps organization named Contoso.

You need to receive Microsoft Teams notifications when work items are updated.

What should you do?

- A. From Azure DevOps, configure a service hook subscription
- B. From Microsoft Teams, configure a connector
- C. From Microsoft Teams admin center, configure external access
- D. From Microsoft Teams, add a channel

E. From Azure DevOps, install an extension

Answer: A

Explanation:

Service hooks let you run tasks on other services when events happen in your Azure DevOps projects. For example, create a card in Trello when a work item is created or send a push notification to your team's mobile devices when a build fails. You can also use service hooks in custom apps and services as a more efficient way to drive activities when events happen in your projects.

Note: Service hook publishers define a set of events. Subscriptions listen for the events and define actions to take based on the event. Subscriptions also target consumers, which are external services that can run their own actions, when an event occurs.

Reference:

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

QUESTION 252

You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 that is configured for autoscaling.

You use Azure DevOps to build a web app named App1 and deploy App1 to VMSS1. App1 is used heavily and has usage patterns that vary on a weekly basis.

You need to recommend a solution to detect an abnormal rise in the rate of failed requests to App1. The solution must minimize administrative effort.

What should you include in the recommendation?

- A. the Smart Detection feature in Azure Application Insights
- B. the Failures feature in Azure Application Insights
- C. an Azure Service Health alert
- D. an Azure Monitor alert that uses an Azure Log Analytics query

Answer: A

Explanation:

After setting up Application Insights for your project, and if your app generates a certain minimum amount of data, Smart Detection of failure anomalies takes 24 hours to learn the normal behavior of your app, before it is switched on and can send alerts.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-failure-diagnostics>

QUESTION 253

You create an alert rule in Azure Monitor as shown in the following exhibit.

Create rule

Rules management

*** RESOURCE**



ASP-9bb7

Select

HIERARCHY



Contoso > CoreApp1

*** CONDITION**



Whenever the Activity Log has an event with Category='Administrative', Signal name='All Administrative operations', Status='failed'

Add

Azure Alerts are currently limited to either 2 metric, 1 log, or 1 activity log signal per alert rule. To alert on more signals, please create additional alert rules.

ACTIONS GROUPS (optional)



Action group name	Contain actions
Application Insights Smart Detection	2 Email Azure Resource Manager Role(s)

Add Create

Action rules (preview) allows you to define actions at scale as well as suppress actions. Learn more about this functionality by clicking on this banner.

Which action will trigger an alert?

- A. a failed attempt to delete the ASP-9bb7 resource
- B. a change to a role assignment for the ASP-9bb7 resource
- C. a successful attempt to delete the ASP-9bb7 resource
- D. a failed attempt to scale up the ASP-9bb7 resource

Answer: A

QUESTION 254

You have a web app hosted on Azure App Service. The web app stores data in an Azure SQL database.

You need to generate an alert when there are 10,000 simultaneous connections to the database. The solution must minimize development effort.

Which option should you select in the Diagnostics settings of the database?

- A. Send to Log Analytics
- B. Stream to an event hub
- C. Archive to a storage account

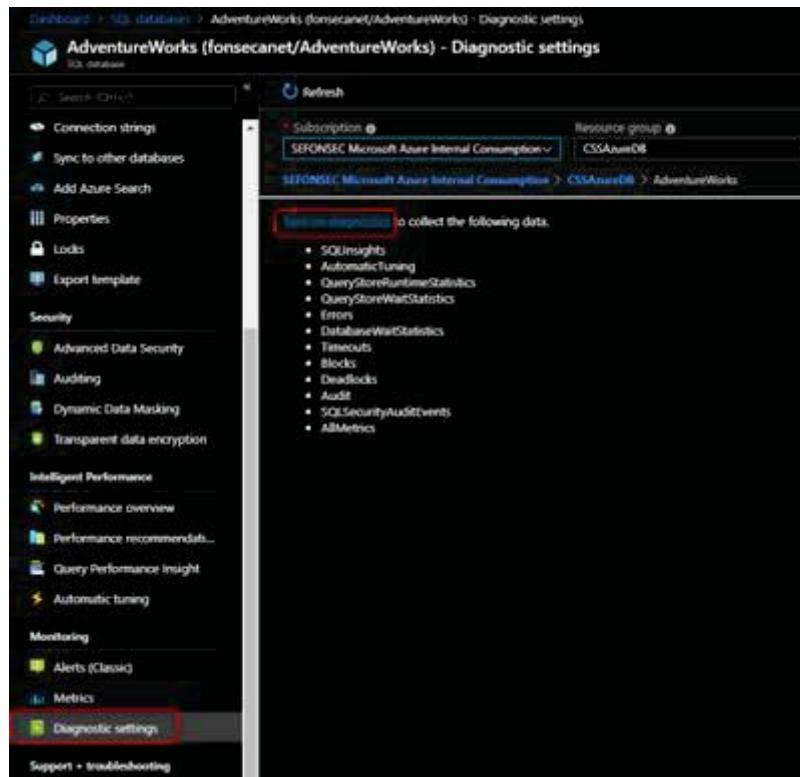
Answer: A

Explanation:

ENABLE DIAGNOSTICS TO LOG ANALYTICS

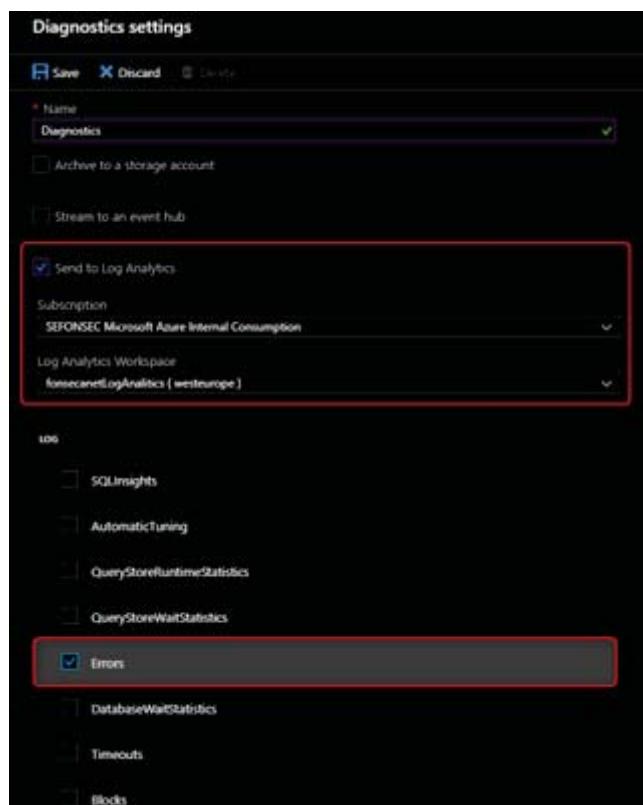
This configuration is done PER DATABASE

1. Click on Diagnostics Settings and then Turn On Diagnostics



The screenshot shows the Azure portal interface for managing diagnostic settings for the AdventureWorks database. The left sidebar includes sections for Connection string, Sync to other databases, Add Azure Search, Properties (Locks, Export template), Security (Advanced Data Security, Auditing, Dynamic Data Masking, Transparent data encryption), Intelligent Performance (Performance overview, Performance recommendations, Query Performance Insight, Automatic tuning), Monitoring (Alerts (Classic), Metrics, Diagnostic settings), and Support + troubleshooting. The 'Metrics' section is currently selected. The main pane displays the 'Subscription' dropdown set to 'SEFONSEC Microsoft Azure Internal Consumption', the 'Resource group' dropdown set to 'CSSAzureDB', and the 'Log Analytics workspace' dropdown set to 'fonscanetLogAnalytics (westeurope)'. A red box highlights the 'Diagnostic settings' button at the bottom of the sidebar.

2. Select to Send to Log Analytics and select the Log Analytics workspace. For this sample I will selected only Errors



The screenshot shows the 'Diagnostics settings' configuration page. It includes fields for 'Name' (set to 'Diagnostics'), 'Archive to a storage account', and 'Stream to an event hub'. The 'Send to Log Analytics' checkbox is checked. The 'Subscription' dropdown is set to 'SEFONSEC Microsoft Azure Internal Consumption'. The 'Log Analytics Workspace' dropdown is set to 'fonscanetLogAnalytics (westeurope)'. The 'LOG' section contains several checkboxes: 'SQLInsights', 'AutomaticTuning', 'QueryStoreRuntimeStatistics', 'QueryStoreWaitStatistics', 'Errors' (which is checked and highlighted by a red box), 'DatabaseWaitStatistics', 'Timeouts', and 'Blocks'.

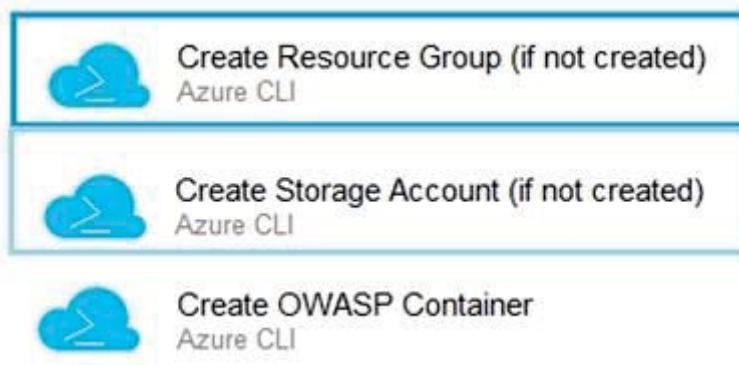
Reference:

<https://techcommunity.microsoft.com/t5/azure-database-support-blog/azure-sql-db-and-log-analytics-better-together-part-1/ba-p/794833>

QUESTION 255

Drag and Drop Question

You have an Azure DevOps release pipeline as shown in the following exhibit.



You need to complete the pipeline to configure OWASP ZAP for security testing.

Which five Azure CLI tasks should you add in sequence? To answer, move the tasks from the list of tasks to the answer area and arrange them in the correct order.

Tasks	Answer Area
Convert Report Format	
Build machine image	
Publish Test Results	↗
Destroy OWASP Container	↖ ↘
Call the Baseline Scan	
Docker CLI installer	
Download the file	↑ ↓

Answer:

Tasks

Build machine image

Docker CLI installer

Answer Area

Call the Baseline Scan

Download the file

Convert Report Format

Publish Test Results

Destroy OWASP Container

**Explanation:**

Defining the Release Pipeline

Once the application portion of the Release pipeline has been configured, the security scan portion can be defined. In our example, this consists of 8 tasks, primarily using the Azure CLI task to create and use the ACI instance (and supporting structures).

Otherwise specified, all the Azure CLI tasks are Inline tasks, using the default configuration options.

 Create Resource Group (if not created)	<input checked="" type="checkbox"/>	
 Create Storage Account (if not created)	<input type="radio"/>	
 Create OWASP Container		
Azure CLI		
 Call the Baseline Scan		
Azure CLI		
 Download the file		
Azure CLI		
 Convert Report Format		
PowerShell		
 Publish Test Results		
Publish Test Results		
 Destroy OWASP Container		
Azure CLI		

Reference:

<https://devblogs.microsoft.com/premier-developer/azure-devops-pipelines-leveraging-owasp-zap-in-the-release-pipeline/>

QUESTION 256

Hotspot Question

You company uses a Git source-code repository.

You plan to implement Gitflow as a workflow strategy.

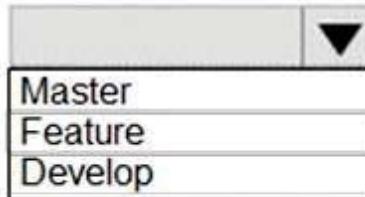
You need to identify which branch types are used for production code and preproduction code in the strategy.

Which branch type should you identify for each code type? To answer, select the appropriate options in the answer area.

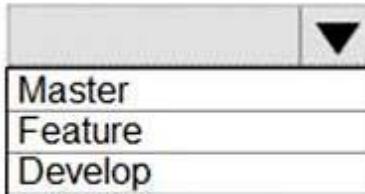
NOTE: Each correct selection is worth one point.

Answer Area

Production code:



Preproduction code:



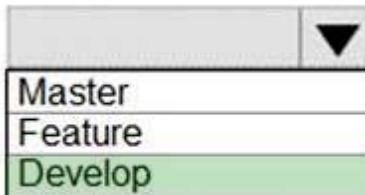
Answer:

Answer Area

Production code:



Preproduction code:



Explanation:

Box 1: Master

The Master branch contains production code. All development code is merged into master in sometime.

Box 2: Develop

The Develop branch contains pre-production code. When the features are finished then they are merged into develop.

Incorrect Answers:

During the development cycle, a variety of supporting branches are used:

Feature branches are used to develop new features for the upcoming releases. May branch off from develop and must merge into develop.

Reference:

<https://medium.com/@patrickporto/4-branching-workflows-for-git-30d0aaee7bf>

QUESTION 257

Drag and Drop Question

You have an Azure subscription that contains a resources group named RG1. RG1 contains the following resources:

- Four Azure virtual machines that run Windows Server and have Internet Services (IIS) installed.
- SQL Server on an Azure virtual machine.
- An Azure Load Balancer.

You need to deploy an application to the virtual machines in RG1 by using Azure Pipelines.

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.

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

Actions	Answer Area
Create an agent pool	
Add the Puppet Agent extension to the virtual machines	
Add and configure a deployment group job for the pipeline	
Execute the Azure Pipelines Agent extension to the virtual machines	  
Create a deployment group	

Answer:

Actions

Add the Puppet Agent extension to the virtual machines

Answer Area

Create an agent pool

Create a deployment group



Execute the Azure Pipelines Agent extension to the virtual machines

Add and configure a deployment group job for the pipeline

**Explanation:**

Step 1: Create an agent pool

Azure Pipelines provides a pre-defined agent pool named Azure Pipelines with Microsoft-hosted agents.

Step 2: Create a deployment group

Deployment groups make it easy to define logical groups of target machines for deployment, and install the required agent on each machine.

Step 3: Execute the Azure Pipelines Agent extension to the virtual machines
Install the Azure Pipelines Agent Azure VM extension

Step 4: Add and configure a deployment group job for the pipeline
Tasks that you define in a deployment group job run on some or all of the target servers, depending on the arguments you specify for the tasks and the job itself.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deployment-groups/how-to-provision-deployment-group-agents>

QUESTION 258

Hotspot Question

You have an application named App1 that has a custom domain of app.contoso.com.

You create a test in Azure Application Insights as shown in the following exhibit.

Create test

Basic Information

* Test name

 ✓

Learn more about configuring tests against applications hosted behind a firewall

Test type

 ▼

* URL ⓘ

 ✓

Parse dependent requests ⓘ



Enable retries for availability test failures. ⓘ



Test frequency ⓘ

 ▼

Test locations

4 location(s) configured

Success criteria

Test Timeout ⓘ

 ▼

Status code must equal



Content must contain

Alerts

Enabled

Create

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.

Answer Area

The test will execute [answer choice].

every 30 seconds at a random location
every 30 seconds per location
every five minutes at a random location
every five minutes per location

The test will pass if [answer choice] within 30 seconds.

App1 responds to an ICMP ping
the HTML of App1 and the HTML from URLs in <a> tags load all the HTML, JavaScripts, and images of App1 load

Answer:

Answer Area

The test will execute [answer choice].

every 30 seconds at a random location
every 30 seconds per location
every five minutes at a random location
every five minutes per location

The test will pass if [answer choice] within 30 seconds.

App1 responds to an ICMP ping
the HTML of App1 and the HTML from URLs in <a> tags load all the HTML, JavaScripts, and images of App1 load

Explanation:

Box 1: every five minutes at a random location

Test frequency: Sets how often the test is run from each test location. With a default frequency of five minutes and five test locations, your site is tested on average every minute.

Box 2:

Parse dependent requests: Test requests images, scripts, style files, and other files that are part of the web page under test. The recorded response time includes the time taken to get these files. The test fails if any of these resources cannot be successfully downloaded within the timeout for the whole test.

Reference:

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

QUESTION 259

Hotspot Question

You use Azure Pipelines to manage the build and deployment of apps.

You are planning the release strategies for a new app.

You need to choose strategies for the following scenarios:

- Releases will be made available to users who are grouped by their tolerance for software faults.
- Code will be deployed to enable functionality that will be available in later releases of the app.
- When a new release occurs, the existing deployment will remain active to minimize recovery time if a return to the previous version is required.

Which strategy should you choose for each scenario? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Releases will be made available to users who are grouped by their tolerance for software faults:

▼
Progressive exposure
Blue/green
Feature flags

Code will be deployed to enable functionality that will be available in later releases of the app:

▼
Progressive exposure
Blue/green
Feature flags

When a new release occurs, the existing deployment will remain active to minimize recovery time if a return to the previous version is required:

▼
Progressive exposure
Blue/green
Feature flags

Answer:

Answer Area

Releases will be made available to users who are grouped by their tolerance for software faults:

▼
Progressive exposure
Blue/green
Feature flags

Code will be deployed to enable functionality that will be available in later releases of the app:

▼
Progressive exposure
Blue/green
Feature flags

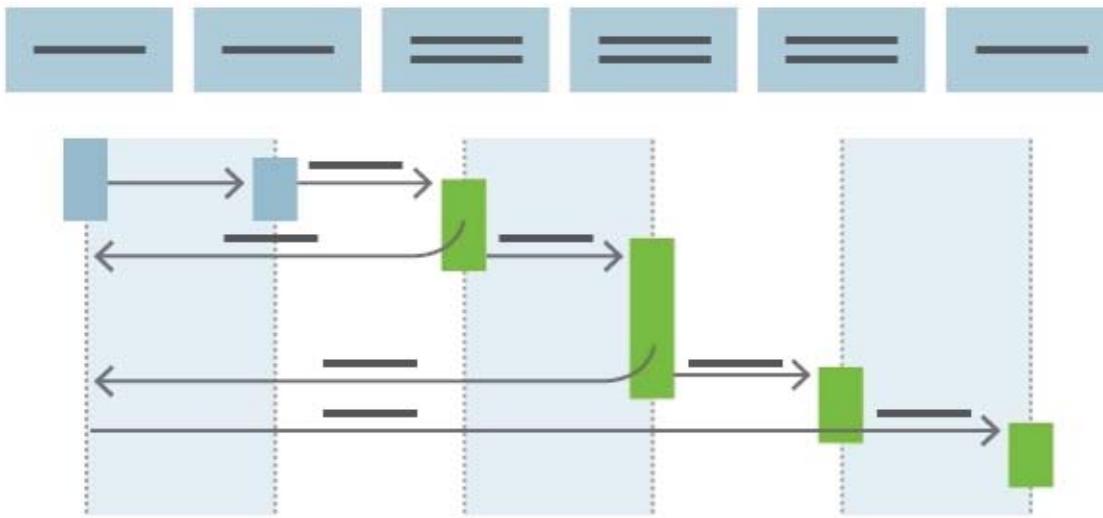
When a new release occurs, the existing deployment will remain active to minimize recovery time if a return to the previous version is required:

▼
Progressive exposure
Blue/green
Feature flags

Explanation:

Box 1: Progressive exposure

Continuous Delivery may sequence multiple deployment "rings" for progressive exposure (also known as "controlling the blast radius"). Progressive exposure groups users who get to try new releases to monitor their experience in "rings." The first deployment ring is often a "canary" used to test new versions in production before a broader rollout. CD automates deployment from one ring to the next and may optionally depend on an approval step, in which a decision maker signs off on the changes electronically. CD may create an auditable record of the approval in order to satisfy regulatory procedures or other control objectives.


Box 2: Feature flags

Feature flags support a customer-first DevOps mindset, to enable (expose) and disable (hide) features in a solution, even before they are complete and ready for release.

Box 3: Blue/green

Blue/green deployments which means that instead of replacing the previous version (here we refer to this version as blue), we bring up the new version (here referred to as the green version) next to the existing version, but not expose it to the actual users right away. On the condition of having successfully validated that the green version works correctly, we will promote this version to the public version by changing the routing configuration without downtime. If something is wrong with the green version we can revert back without users every noticing interruptions.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/learn/what-is-continuous-delivery>
<https://docs.microsoft.com/en-us/azure/devops/migrate/phase-features-with-feature-flags>
<https://medium.com/@denniszielke/continuous-kubernetes-blue-green-deployments-on-azure-using-nginx-appgateway-or-trafficmanager-4490bce29cb>

QUESTION 260

Drag and Drop Question

You have a project in Azure DevOps.

You need to associate an automated test to a test case.

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	Answer Area
Debug the project	
Create a test project	
Create a work item	▶
Check in a project to the Azure DevOps repository	◀
Add the automated test to a build pipeline	

Answer:

Actions	Answer Area
Debug the project	Create a test project
	Check in a project to the Azure DevOps repository
Create a work item	▶
	Add the automated test to a build pipeline

Explanation:

The process to associate an automated test with a test case is:

1. Create a test project containing your automated test. What types of tests are supported?
2. Check your test project into an Azure DevOps or Team Foundation Server (TFS) repository.
3. Create a build pipeline for your project, ensuring that it contains the automated test. What are the differences if I am still using a XAML build?
4. Use Visual Studio Enterprise or Professional 2017 or a later version to associate the automated test with a test case as shown below. The test case must have been added to a test plan that uses the build you just defined.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/test/associate-automated-test-with-test-case>

QUESTION 261

Drag and Drop Question

Your company has two virtual machines that run Linux in a third-party public cloud.

You plan to use the company's Azure Automation State Configuration implementation to manage the two virtual machines and detect configuration drift.

You need to onboard the Linux virtual machines.

You install PowerShell Desired State Configuration (DSC) on the virtual machines, and then run register.py

Which three actions should you perform next in sequence? To answer, move the actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Create a DSC metaconfiguration	
Copy the metaconfiguration to the virtual machines	
Add the virtual machines as DSC nodes in Azure Automation	
Install Windows Management Framework 5.1 on the virtual machines	
From the virtual machines, run setdsclocalconfigurationmanager.py	

Answer:

Actions	Answer Area
	Create a DSC metaconfiguration
	Copy the metaconfiguration to the virtual machines
	Add the virtual machines as DSC nodes in Azure Automation
Install Windows Management Framework 5.1 on the virtual machines	
From the virtual machines, run setdsclocalconfigurationmanager.py	

Explanation:



Step 1: Create a DSC metaconfiguration

Load up the DSC Configuration into Azure Automation.

Step 2: Copy the metaconfiguration to the virtual machines.

Linking the Node Configuration to the Linux Host

Step 3: Add the virtual machines as DSC nodes in Azure Automation. go to DSC Nodes, select your node, and then click Assign node configuration. This step assigns the DSC configuration to the Linux machine.

Next up will be to link the node configuration to the host. Go to the host and press the "Assign node..."- button. Next up you can select your node configuration.

QUESTION 262

Hotspot Question

Your company uses Azure DevOps for Git source control.

You have a project in Azure DevOps named Contoso App that contains the following repositories:

<https://dev.azure.com/contoso/contoso-app/core-api>
<https://dev.azure.com/contoso/contoso-app/core-spa>
<https://dev.azure.com/contoso/contoso-app/core-db>

You need to ensure that developers receive Slack notifications when there are pull requests created for Contoso App.

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

NOTE: Each correct selection is worth one point.

Answer Area

/azrepos	feedback
	signin
	subscribe
	subscriptions

https://dev.azure.com/contoso/contoso-app
https://dev.azure.com/contoso/contoso-app/core-api
https://dev.azure.com/contoso/contoso-app/core-db
https://dev.azure.com/contoso/contoso-app/core-spa

Answer:

Answer Area

/azrepos	feedback
	signin
	subscribe
	subscriptions

https://dev.azure.com/contoso/contoso-app
https://dev.azure.com/contoso/contoso-app/core-api
https://dev.azure.com/contoso/contoso-app/core-db
https://dev.azure.com/contoso/contoso-app/core-spa

Explanation:

Box 1: subscribe

To start monitoring all Git repositories in a project, use the following slash command inside a channel:

/azrepos subscribe [project url]

Box 2: <https://dev.azure.com/contoso/contoso-app>

You can also monitor a specific repository using the following command:

/azrepos subscribe [repository url]

The repository URL can be to any page within your repository that has your repository name.

For example, for Git repositories, use:

/azrepos subscribe https://dev.azure.com/myorg/myproject/_git/myrepository

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/integrations/repos-slack>

QUESTION 263

Hotspot Question

You use Azure DevOps to manage the build and deployment of an app named App1.

You have release pipeline that deploys a virtual machine named VM1.

You plan to monitor the release pipeline by using Azure Monitor.

You need to create an alert to monitor the performance of VM1. The alert must be triggered when the average CPU usage exceeds 70 percent for five minutes. The alert must calculate the average once every minute.

How should you configure the alert rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Aggregation granularity (Period):

1 minute
5 minutes

Threshold value:

Static
Dynamic

Operator:

Greater than
Greater than or equal to
Less than or equal to
Less than

Answer:

Answer Area

Aggregation granularity (Period):

1 minute	▼
5 minutes	

Threshold value:

Static	▼
Dynamic	

Operator:

Greater than	▼
Greater than or equal to	
Less than or equal to	
Less than	

Explanation:

Box 1: 5 minutes

The alert must calculate the average once every minute.

Note: We [Microsoft] recommend choosing an Aggregation granularity (Period) that is larger than the Frequency of evaluation, to reduce the likelihood of missing the first evaluation of added time series

Box 2: Static

Box 3: Greater than

Example, say you have an App Service plan for your website. You want to monitor CPU usage on multiple instances running your web site/app. You can do that using a metric alert rule as follows:

Target resource: myAppServicePlan

Metric: Percentage CPU

Condition Type: Static

Dimensions

Instance = InstanceName1, InstanceName2

Time Aggregation: Average

Period: Over the last 5 mins

Frequency: 1 min

Operator: GreaterThan

Threshold: 70

Like before, this rule monitors if the average CPU usage for the last 5 minutes exceeds 70%.

Aggregation granularity

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric-overview>

QUESTION 264

Hotspot Question

You have an Azure Kubernetes Service (AKS) pod.

You need to configure a probe to perform the following actions:

- Confirm that the pod is responding to service requests.
- Check the status of the pod four times a minute.
- Initiate a shutdown if the pod is unresponsive.

How should you complete the YAML configuration file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
apiVersion: v1
kind: Pod
metadata:
  labels:
    test: readiness-and-liveness
    name: readiness-http
spec:
  containers:
  - name: container1
    image: k8s.gcr.io/readiness-and-liveness
    args:
    - /server

  livenessProbe:
  readinessProbe:
  ShutdownProbe:
  startupProbe:

  httpGet:
    path: /checknow
    port: 8123
    httpHeaders:
    - name: Custom-Header
      value: CheckNow
```

initialDelaySeconds: 15
periodSeconds: 15
timeoutSeconds: 15

Answer:

Answer Area

```
apiVersion: v1
kind: Pod
metadata:
  labels:
    test: readiness-and-liveness
    name: readiness-http
spec:
  containers:
    - name: container1
      image: k8s.gcr.io/readiness-and-liveness
      args:
        - /server
      livenessProbe:
        httpGet:
          path: /checknow
          port: 8123
          httpHeaders:
            - name: Custom-Header
              value: CheckNow
```

livenessProbe:
readinessProbe:
ShutdownProbe:
startupProbe:

initialDelaySeconds: 15
periodSeconds: 15
timeoutSeconds: 15

Explanation:

Box 1: readinessProbe:

For containerized applications that serve traffic, you might want to verify that your container is ready to handle incoming requests. Azure Container Instances supports readiness probes to include configurations so that your container can't be accessed under certain conditions.

Incorrect Answers:

livenessProbe: Containerized applications may run for extended periods of time, resulting in broken states that may need to be repaired by restarting the container. Azure Container Instances supports liveness probes so that you can configure your containers within your container group to restart if critical functionality is not working.

Box 2: periodSeconds: 15

The periodSeconds property designates the readiness command should execute every 15 seconds.

Reference:

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-readiness-probe>

QUESTION 265

You have an Azure DevOps organization named Contoso.

You need to recommend an authentication mechanism that meets the following requirements:

- Supports authentication from Git
- Minimizes the need to provide credentials during authentication

What should you recommend?

- A. personal access tokens (PATs) in Azure DevOps
- B. Alternate credentials in Azure DevOps
- C. user accounts in Azure Active Directory (Azure AD)
- D. managed identities in Azure Active Directory (Azure AD)

Answer: A

Explanation:

Personal access tokens (PATs) give you access to Azure DevOps and Team Foundation Server (TFS), without using your username and password directly. These tokens have an expiration date from when they're created. You can restrict the scope of the data they can access. Use PATs to authenticate if you don't already have SSH keys set up on your system or if you need to restrict the permissions that are granted by the credential.

Incorrect Answers:

B: Azure DevOps no longer supports Alternate Credentials authentication since the beginning of March 2, 2020. If you're still using Alternate Credentials, we [Microsoft] strongly encourage you to switch to a more secure authentication method (for example, personal access tokens).

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/auth-overview>

QUESTION 266

You plan to onboard 10 new developers.

You need to recommend a development environment that meets the following requirements:

- Integrates with GitHub
- Provides integrated debugging tools
- Supports remote workers and hot-desking environments
- Supports developers who use browsers, tablets, and Chromebooks

What should you recommend?

- A. VS Code
- B. Xamarin Studio
- C. MonoDevelop
- D. Visual Studio Codespaces

Answer: D

Explanation:

Visual Studio Codespaces is built to accommodate the widest variety of projects or tasks, including GitHub and integrating debugging.

Visual Studio Codespaces conceptually and technically extends the Visual Studio Code Remote Development extensions.

In addition to "backend" environments, Visual Studio Codespaces supports these "frontend"

editors:

- Visual Studio Code
- Visual Studio Code-based editor in the browser

Reference:

<https://docs.microsoft.com/sv-se/visualstudio/codespaces/overview/what-is-vsonline>

QUESTION 267

You have an Azure subscription that contains resources in several resource groups.

You need to design a monitoring strategy that will provide a consolidated view. The solution must support the following requirements:

- Support role-based access control (RBAC) by using Azure Active Directory (Azure AD) identities.
- Include visuals from Azure Monitor that are generated by using the Kusto query language.
- Support documentation written in markdown.
- Use the latest data available for each visual.

What should you use to create the consolidated view?

- A. Azure Monitor
- B. Microsoft Power BI
- C. Azure Data Explorer
- D. Azure dashboards

Answer: 

Explanation: 

There are several tools available for running queries in Azure Data Explorer, including Kusto. Kusto uses a role-based access control (RBAC) model, under which authenticated principals are mapped to roles, and get access according to the roles they're assigned.

Note: Azure Data Explorer is a highly scalable and secure analytics service that enables you to do rich exploration of structured and unstructured data for instant insights. Optimized for ad-hoc queries, Azure Data Explorer enables rich data exploration over raw, structured, and semi-structured data delivering fast time to insight. Query with a modern, intuitive query language that offers fast, ad-hoc, and advanced query capabilities over high-rate data volumes and varieties

Reference:

<https://docs.microsoft.com/en-us/azure/data-explorer/tools-integrations-overview>

QUESTION 268

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 coupling and the dependency cycles?

Does this meet the goal?

- A. Yes
- B. No

Answer: 

Explanation:

Instead reduce the code complexity.

Note: Technical debt is the accumulation of sub-optimal technical decisions made over the lifetime of an application. Eventually, it gets harder and harder to change things: it's the 'sand in the gears' that sees IT initiatives grind to a halt.

Reference:

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

<https://www.devopsgroup.com/blog/five-ways-devops-helps-with-technical-debt/>

QUESTION 269

You are building an ASP.NET Core application.

You plan to create an application utilization baseline by capturing telemetry data.

You need to add code to the application to capture the telemetry data. The solution must minimize the costs of storing the telemetry data.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point

- A. Add the <InitialSamplingPercentage>99</InitialSamplingPercentage> parameter to the ApplicationInsights.config file.
- B. From the code of the application, enable adaptive sampling.
- C. From the code of the application, add Azure Application Insights telemetry.
- D. Add the <MaxTelemetryItemsPerSecond>5</MaxTelemetryItemsPerSecond> parameter to the ApplicationInsights.config file.
- E. From the code of the application, disable adaptive sampling.

Answer: 

Explanation:

Sampling is a feature in Azure Application Insights. It is the recommended way to reduce telemetry traffic, data costs, and storage costs, while preserving a statistically correct analysis of application data.

The Application Insights SDK for ASP.NET Core supports both fixed-rate and adaptive sampling. Adaptive sampling is enabled by default.

D: For adaptive sampling: The volume is adjusted automatically to keep within a specified maximum rate of traffic, and is controlled via the setting MaxTelemetryItemsPerSecond. If the application produces a low amount of telemetry, such as when debugging or due to low usage, items won't be dropped by the sampling processor as long as volume is below MaxTelemetryItemsPerSecond.

Note: In ApplicationInsights.config, you can adjust several parameters in the AdaptiveSamplingTelemetryProcessor node. The figures shown are the default values:

<MaxTelemetryItemsPerSecond>5</MaxTelemetryItemsPerSecond>

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/sampling>

QUESTION 270

You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 and an Azure Standard Load Balancer named LB1. LB1 distributes incoming requests across VMSS1 instances.

You use Azure DevOps to build a web app named App1 and deploy App1 to VMSS1. App1 is accessible via HTTPS only and configured to require mutual authentication by using a client certificate.

You need to recommend a solution for implementing a health check of App1. The solution must meet the following requirements:

Identify whether individual instances of VMSS1 are eligible for an upgrade operation.
Minimize administrative effort.

What should you include in the recommendation?

- A. an Azure Load Balancer health probe
- B. Azure Monitor autoscale
- C. the Custom Script Extension
- D. the Application Health extension

Answer: D

Explanation:

Monitoring your application health is an important signal for managing and upgrading your deployment.

Azure virtual machine scale sets provide support for rolling upgrades including automatic OS-image upgrades, which rely on health monitoring of the individual instances to upgrade your deployment. You can also use health extension to monitor the application health of each instance in your scale set and perform instance repairs using automatic instance repairs.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-health-extension>

QUESTION 271

You have an existing build pipeline in Azure Pipelines.

You need to use incremental builds without purging the environment between pipeline executions.

What should you use?

- A. a self-hosted agent
- B. Microsoft-hosted parallel jobs
- C. a File Transform task

Answer: A

Explanation:

When you run a pipeline on a self-hosted agent, by default, none of the subdirectories are cleaned in between two consecutive runs. As a result, you can do incremental builds and deployments, provided that tasks are implemented to make use of that. You can override this behavior using the workspace setting on the job.

Incorrect Answers:

B: The workspace clean options are applicable only for self-hosted agents. When using Microsoft-hosted agents, jobs are always run on a new agent.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/process/phases>

QUESTION 272

You manage an Azure web app that supports an e-commerce website.

You need to increase the logging level when the web app exceeds normal usage patterns. The solution must minimize administrative overhead.

Which two resources should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. an Azure Automation runbook
- B. an Azure Monitor alert that has a dynamic threshold
- C. an Azure Monitor alert that has a static threshold
- D. the Azure Monitor autoscale settings
- E. an Azure Monitor alert that uses an action group that has an email action

Answer: AB**Explanation:**

B: Metric Alert with Dynamic Thresholds detection leverages advanced machine learning (ML) to learn metrics' historical behavior, identify patterns and anomalies that indicate possible service issues. It provides support of both a simple UI and operations at scale by allowing users to configure alert rules through the Azure Resource Manager API, in a fully automated manner.

A: You can use Azure Monitor to monitor base-level metrics and logs for most services in Azure. You can call Azure Automation runbooks by using action groups or by using classic alerts to automate tasks based on alerts.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-dynamic-thresholds>

<https://docs.microsoft.com/en-us/azure/automation/automation-create-alert-triggered-runbook>

QUESTION 273

You have a build pipeline in Azure Pipelines that occasionally fails.

You discover that a test measuring the response time of an API endpoint causes the failures.

You need to prevent the build pipeline from failing due to the test.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

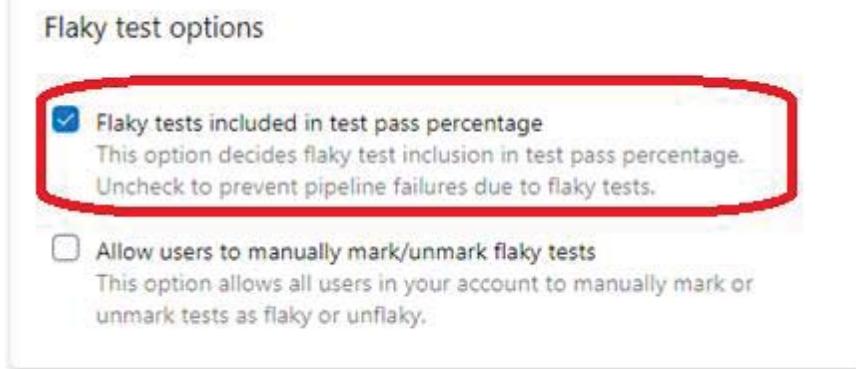
- A. Set Flaky test detection to Off.
- B. Clear Flaky tests included in test pass percentage.
- C. Enable Test Impact Analysis (TIA).
- D. Manually mark the test as flaky.
- E. Enable test slicing.

Answer: BD

Explanation:

D: You can mark or unmark a test as flaky based on analysis or context, by choosing Flaky. To configure flaky test management, choose Project settings, and select Test management in the Pipelines section.

B: Slide the On/Off button to On.



Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/test/flaky-test-management>

QUESTION 274

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 an Octopus Deploy server. You deploy a polled Tentacle agent to an on-premises server. You add an Octopus 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).

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops>

QUESTION 275

You have an Azure DevOps project named Project1 and an Azure subscription named Sub1.

You need to prevent releases from being deployed unless the releases comply with the Azure Policy rules assigned to Sub1.

What should you do in the release pipeline of Project1?

- A. Add a deployment gate.
- B. Modify the Deployment queue settings.
- C. Configure a deployment trigger.
- D. Create a pipeline variable.

Answer: A

Explanation:

You can check policy compliance with gates.

You can extend the approval process for the release by adding a gate. Gates allow you to configure automated calls to external services, where the results are used to approve or reject a deployment.

You can use gates to ensure that the release meets a wide range of criteria, without requiring user intervention.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deploy-using-approvals>

QUESTION 276

You have a project in Azure DevOps named Project1. Project1 contains a build pipeline named Pipe1 that builds an application named App1.

You have an agent pool named Pool1 that contains a Windows Server 2019-based self-hosted agent.

Pipe1 uses Pool1.

You plan to implement another project named Project2. Project2 will have a build pipeline named Pipe2 that builds an application named App2.

App1 and App2 have conflicting dependencies.

You need to minimize the possibility that the two build pipelines will conflict with each other. The solution must minimize infrastructure costs.

What should you do?

- A. Add another self-hosted agent.
- B. Adds Docker Compose task to the build pipelines.
- C. Change the self-hosted agent to use Red Hat Enterprise Linux (RHEL) 8.
- D. Create two container jobs.

Answer: D

Explanation:

To get more control over software dependencies and operating system, you can use Container jobs. Note that the decisions whether to run your pipeline inside a container and whether to use a self-hosted agent are independent. You can directly run your pipeline on a self-hosted agent, or inside a container. You can also execute your pipeline in a container on a Microsoft-hosted agent or on a self-hosted agent.

Incorrect Answers:

A: For additional control over hardware, you can use a self-hosted build agent.

Reference:

<http://thewindowsupdate.com/2019/09/09/resolving-complex-software-and-hardware-dependencies-in-azure-devops-pipelines/>

QUESTION 277

You have an Azure DevOps project that uses many package feeds.

You need to simplify the project by using a single feed that stores packages produced by your company and packages consumed from remote feeds. The solution must support public feeds and authenticated feeds.

What should you enable in DevOps?

- A. Universal Packages
- B. upstream sources
- C. views in Azure Artifacts
- D. a symbol server

Answer: B

Explanation:

Upstream sources enable you to use a single feed to store both the packages you produce and the packages you consume from "remote feeds". This includes both public feeds, such as npmjs.com and nuget.org, and authenticated feeds, such as other Azure DevOps feeds in your organization. Once you've enabled an upstream source, any user connected to your feed can install a package from the remote feed, and your feed will save a copy.

Reference:

<https://azure.microsoft.com/en-us/blog/deep-dive-into-azure-artifacts/>

QUESTION 278

You are monitoring the health and performance of an Azure web app by using Azure Application Insights.

You need to ensure that an alert is sent when the web app has a sudden rise in performance issues and failures.

What should you use?

- A. custom events
- B. Application Insights Profiler
- C. usage analysis
- D. Smart Detection
- E. Continuous export

Answer: D

Explanation:

Smart Detection automatically warns you of potential performance problems and failure anomalies in your web application. It performs proactive analysis of the telemetry that your app sends to Application Insights.

If there is a sudden rise in failure rates, or abnormal patterns in client or server performance, you get an alert.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-diagnostics>

QUESTION 279

You have a build pipeline in Azure Pipelines.

You create a Slack App Integration.

You need to send build notifications to a Slack channel named #Development.

What should you do first?

- A. Create a project-level notification.
- B. Configure a service connection.
- C. Create a global notification.
- D. Creates a service hook subscription.

Answer: D

Explanation:

Create a service hook for Azure DevOps with Slack to post messages to Slack in response to events in your Azure DevOps organization, such as completed builds, code changes, pull requests, releases, work items changes, and more.

Note:

1. Go to your project Service Hooks page:
https://{{orgName}}/{{project_name}}/_settings/serviceHooks Select Create Subscription.
3. Choose the types of events you want to appear in your Slack channel.
4. Paste the Web Hook URL from the Slack integration that you created and select Finish.
5. Now, when the event you configured occurs in your project, a notification appears in your team's Slack channel.

Reference:

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

QUESTION 280

You have a private GitHub repository.

You need to display the commit status of the repository on Azure Boards.

What should you do first?

- A. Configure multi-factor authentication (MFA) for your GitHub account.
- B. Add the Azure Pipelines app to the GitHub repository.
- C. Add the Azure Boards app to the repository.
- D. Create a GitHub action in GitHub.

Answer: C

Explanation:

To connect Azure Boards to GitHub.com, connect and configure from Azure Boards. Or, alternatively, install and configure the Azure Boards app from GitHub. Both methods have been streamlined and support authenticating and operating via the app rather than an individual.

Note (see step 4 below):

Add a GitHub connection:

1. Sign into Azure Boards.
2. Choose (1) Project Settings, choose (2) GitHub connections and then (3) Connect your GitHub account.
3. If this is your first time connecting to GitHub from Azure Boards, you will be asked to sign in using your GitHub credentials. Choose an account for which you are an administrator for the repositories you want to connect to.
4. The Add GitHub Repositories dialog automatically displays and selects all GitHub.com repositories for which you are an administrator. Unselect any repositories that you don't want to participate in the integration.

Add GitHub repositories

X

Add the GitHub repositories you want to use with your Azure Boards.

Filter by keywords X

Viewing 4, 4 selected

-  JamalHart/fabrikam-apps-2
-  JamalHart/fabrikam-demo
-  JamalHart/fabrikam-open-source
-  JamalHart/fabrikam-suite

Save

Reference:

<https://docs.microsoft.com/en-us/azure/devops/boards/github/connect-to-github>

QUESTION 281

Hotspot Question

You manage the Git repository for a large enterprise application.

You need to minimize the data size of the repository.

How should you complete the commands? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

git gc

- aggressive
- auto
- force
- no-prune

git

--expire now

- merge
- prune
- rebase
- reset

Answer:

Answer Area

git gc

- aggressive
- auto
- force
- no-prune

git

--expire now

- merge
- prune
- rebase
- reset

Explanation:

Box 1: --aggressive

Cleanup unnecessary files and optimize the local repository:

```
git gc --aggressive
```

Box 2: prune

Prune all unreachable objects from the object database:

```
git prune
```

Reference:

<https://gist.github.com/Zoramite/2039636>**QUESTION 282**

Drag and Drop Question

You use GitHub Enterprise Server as a source code repository.

You create an Azure DevOps organization named Contoso.

In the Contoso organization, you create a project named Project1.

You need to link GitHub commits, pull requests, and issues to the work items of Project1. The solution must use OAuth-based authentication.

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	Answer Area
From Developer settings in GitHub Enterprise Server, register a new OAuth app.	
From Project Settings in Azure DevOps, create a service hook subscription.	
From Organization settings in Azure DevOps, connect to Azure Active Directory (Azure AD).	 
From Project Settings in Azure DevOps, add a GitHub connection.	
From Organization settings in Azure DevOps, add an OAuth configuration.	
From Developer settings in GitHub Enterprise Server, generate a private key.	

Answer:

Actions	Answer Area
From Project Settings in Azure DevOps, create a service hook subscription.	From Developer settings in GitHub Enterprise Server, register a new OAuth app.
From Organization settings in Azure DevOps, connect to Azure Active Directory (Azure AD).	From Organization settings in Azure DevOps, add an OAuth configuration.
	From Project Settings in Azure DevOps, add a GitHub connection.

From Developer settings in GitHub Enterprise Server, generate a private key.

Explanation:

Step 1: From Developer settings in GitHub Enterprise Server, register a new OAuth app. If you plan to use OAuth to connect Azure DevOps Services or Azure DevOps Server with your GitHub Enterprise Server, you first need to register the application as an OAuth App

Step 2: Organization settings in Azure DevOps, add an OAuth configuration Register your OAuth configuration in Azure DevOps Services.

Note:

1. Sign into the web portal for Azure DevOps Services.
2. Add the GitHub Enterprise Oauth configuration to your organization.
3. Open Organization settings>Oauth configurations, and choose Add Oauth configuration.
4. Fill in the form that appears, and then choose Create.

Step 3: From Project Settings in Azure DevOps, add a GitHub connection. Connect Azure DevOps Services to GitHub Enterprise Server

Choose the Azure DevOps logo to open Projects, and then choose the Azure Boards project you want to configure to connect to your GitHub Enterprise repositories.

Choose (1) Project Settings, choose (2) GitHub connections and then (3) Click here to connect to your GitHub Enterprise organization.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/boards/github/connect-to-github>

QUESTION 283

Drag and Drop Question

You are configuring an Azure DevOps deployment pipeline. The deployed application will authenticate to a web service by using a secret stored in an Azure key vault.

You need to use the secret in the deployment pipeline.

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	Answer Area
Create a service principal in Azure Active Directory (Azure AD).	
Add an app registration in Azure Active Directory (Azure AD).	
Configure an access policy in the key vault.	↶
Generate a self-signed certificate.	↷
Add an Azure Resource Manager service connection to the pipeline.	↑
Export a certificate from the key vault.	↓

Answer:

Actions	Answer Area
	Create a service principal in Azure Active Directory (Azure AD).
Add an app registration in Azure Active Directory (Azure AD).	Configure an access policy in the key vault.
	↶ Add an Azure Resource Manager service connection to the pipeline.
Generate a self-signed certificate.	↷
	↑
Export a certificate from the key vault.	↓

Explanation:


Step 1: Create a service principal in Azure Active Directory (Azure AD). You will need a service principal to deploy an app to an Azure resource from Azure Pipelines.

Step 2: Configure an access policy in the key vault.

You need to secure access to your key vaults by allowing only authorized applications and users. To access the data from the vault, you will need to provide read (Get) permissions to the service principal that you will be using for authentication in the pipeline.

Select Access policy and then select + Add Access Policy to setup a new policy.

[Basics](#) [Access policy](#) [Networking](#) [Tags](#) [Review + create](#)

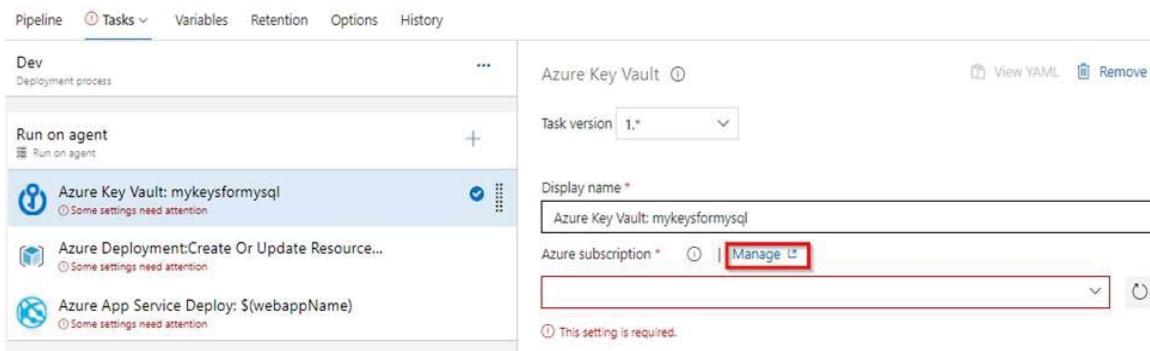
Enable Access to:

- Azure Virtual Machines for deployment ⓘ
- Azure Resource Manager for template deployment ⓘ
- Azure Disk Encryption for volume encryption ⓘ

[+ Add Access Policy](#)

Step 3: Add an Azure Resource Manager service connection to the pipeline You need to authorize the pipeline to deploy to Azure:

1. Select Pipelines | Pipelines,
2. Go to Releases under Pipelines and then select and Edit your pipeline.
3. Under Tasks, notice the release definition for Dev stage has a Azure Key Vault task. This task downloads Secrets from an Azure Key Vault. You will need to point to the subscription and the Azure Key Vault resource.
4. Click Manage, this will redirect to the Service connections page.



The screenshot shows the Azure DevOps Pipeline Task Editor. On the left, there's a list of tasks for a 'Dev' deployment process: 'Run on agent', 'Azure Key Vault: mykeysformysql' (selected), 'Azure Deployment:Create Or Update Resource...', and 'Azure App Service Deploy: \$(webappName)'. The 'Azure Key Vault' task is expanded, showing its configuration. The 'Display name' field is set to 'Azure Key Vault: mykeysformysql'. The 'Azure subscription' dropdown has a red box around the 'Manage' link. A note at the bottom says '(*) This setting is required.'

5. Click on New Service connection -> Azure Resource Manager -> Service Principal (manual). Fill the information from previously created service principal.

Reference:

<https://azuredevopslabs.com/labs/vstsextend/azurekeyvault/>

QUESTION 284

Drag and Drop Question

As part of your application build process, you need to deploy a group of resources to Azure by using an Azure Resource Manager template located on GitHub.

Which three action 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	Answer Area
Set the template parameters.	
Create a package.	
Create a release pipeline.	↖ ↘
Create a job agent.	
Add an Azure Resource Group Deployment task.	↖ ↗

Answer:

Actions	Answer Area
	Create a release pipeline.
Create a package.	
	Add an Azure Resource Group Deployment task.
	↖ ↗ Set the template parameters.
Create a job agent.	

Explanation:

Step 1: Create a release pipeline
You need to create a new pipeline.

You can integrate Azure Resource Manager templates (ARM templates) with Azure Pipelines for continuous integration and continuous deployment (CI/CD).

Step 2: Add an Azure Resource Group Deployment task

Step 3: Set the template parameters

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/add-template-to-azure-pipelines>

QUESTION 285

Drag and Drop Question

You have a project in Azure DevOps that uses packages from multiple public feeds. Some of the feeds are unreliable.

You need to consolidate the packages into a single feed.

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	Answer Area
Modify the configuration files to reference the Azure Artifacts feed.	
Run an initial package restore.	
Create a Microsoft Visual Studio project that includes all the packages.	◀
Create an Azure Artifacts feed that uses upstream sources.	▶
Create a NuGet package.	↑
Create an npm package.	↓

Answer:

Actions	Answer Area
Modify the configuration files to reference the Azure Artifacts feed.	Create a NuGet package.
Run an initial package restore.	Create an Azure Artifacts feed that uses upstream sources.
	Create a Microsoft Visual Studio project that includes all the packages.
	↑
	↓
Create an npm package.	

Explanation:



Step 1: Create a NuGet package.

NuGet and Maven are public package managers that support multiple feeds.

Step 2: Create an Azure Artifacts feed that uses upstream sources If you want to use packages from multiple feeds, use upstream sources to bring packages from multiple feeds together into a single feed.

Step 3: Create a Microsoft Visual Studio project that includes all the packages Consume NuGet packages from upstream sources: Now you can open Visual Studio and install packages from the upstream sources you just configured.

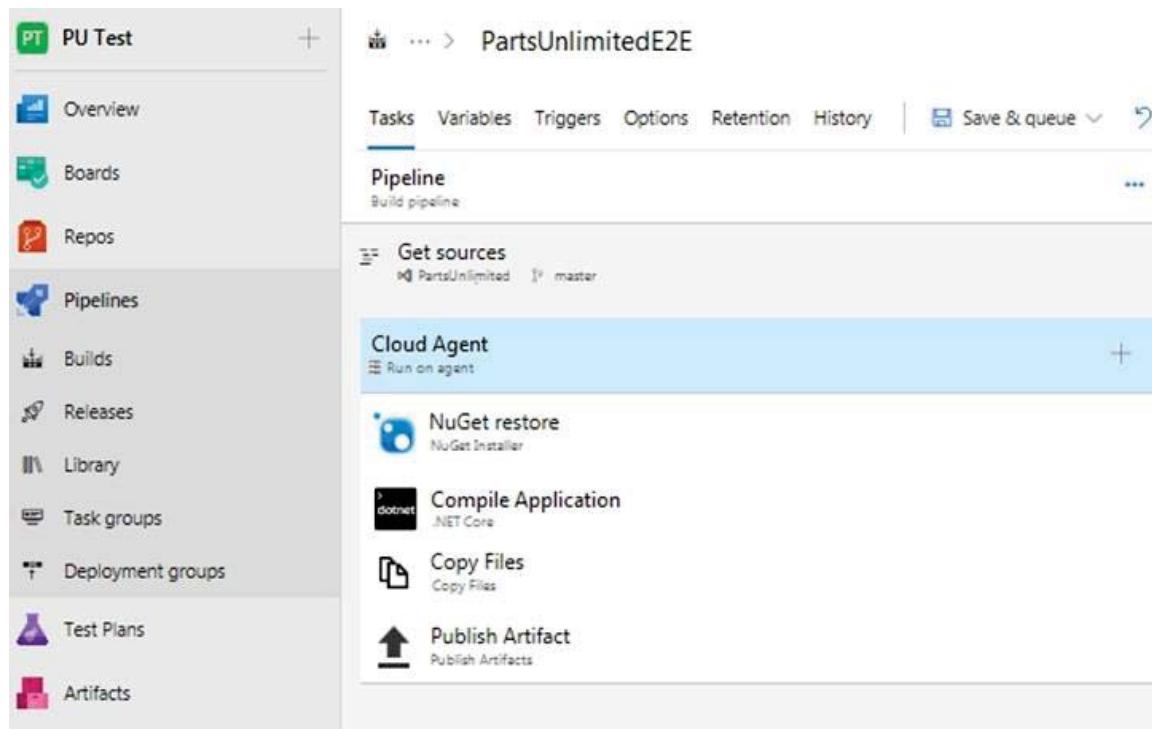
Reference:

<https://docs.microsoft.com/en-us/azure/devops/artifacts/how-to/set-up-upstream-sources>

QUESTION 286

Hotspot Question

You have the Azure DevOps pipeline shown in the following exhibit.



The screenshot shows the Azure DevOps Pipeline interface for the "PU Test" project. The pipeline is named "PartsUnlimitedE2E". The tasks listed are:

- Get sources (Run on agent)
- Cloud Agent (Run on agent) - This task is highlighted with a blue background.
- NuGet restore (NuGet Installer)
- Compile Application (.NET Core)
- Copy Files (Copy Files)
- Publish Artifact (Publish Artifacts)

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.

Answer Area

The pipeline has job(s).

0
1
4

The pipeline has task(s).

0
1
4

Answer:

Answer Area

The pipeline has job(s).

0
1
4

The pipeline has task(s).

0
1
4

Explanation:

Box 1: 1

The Cloud agent job only.

Box 2: 4

The pipelines has the four tasks: NuGet restore, Compile Application, Copy Files, and Publish Artifact.

Reference:

<https://azuredevopslabs.com/labs/azuredevops/continuousintegration/>

QUESTION 287

Drag and Drop Question

You have an Azure DevOps organization named Contoso.

You have 10 Azure virtual machines that run Windows Server 2019. The virtual machines host an application that you build and deploy by using Azure Pipelines. Each virtual machine has the Web Server (IIS) role installed and configured.

You need to ensure that the web server configurations on the virtual machines is maintained automatically. The solution must provide centralized management of the configuration settings and minimize management overhead.

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.

Actions	Answer Area
Create an Azure Automation account.	
Install the custom Desired State Configuration (DSC) extension on the virtual machines.	
Create a .zip file and upload it to Azure Blob storage.	↖
Onboard the virtual machines to the Azure Automation account.	↗
Complete the Desired State Configuration (DSC) configuration.	↙

Answer:

Actions	Answer Area
Create an Azure Automation account.	
Install the custom Desired State Configuration (DSC) extension on the virtual machines.	
Create a .zip file and upload it to Azure Blob storage.	↖
Onboard the virtual machines to the Azure Automation account.	↗
Complete the Desired State Configuration (DSC) configuration.	↙

Explanation:

Step1: Create an Azure Automation account.

An Azure Automation account is required.



Step 2: Install the custom Desired State Configuration (DSC) extension on the virtual machines Under the hood, and without an administrator having to remote into a VM, the Azure VM Desired State Configuration extension registers the VM with Azure Automation State Configuration.

Step 3: Onboard the virtual machines to the Azure Automation account.

Step 4: Complete the Desired State Configuration (DSC) configuration.
Create a DSC configuration.

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-dsc-onboarding>

QUESTION 288

Hotspot Question

You have an Azure web app named Webapp1.

You need to use an Azure Monitor query to create a report that details the top 10 pages of Webapp1 that failed.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

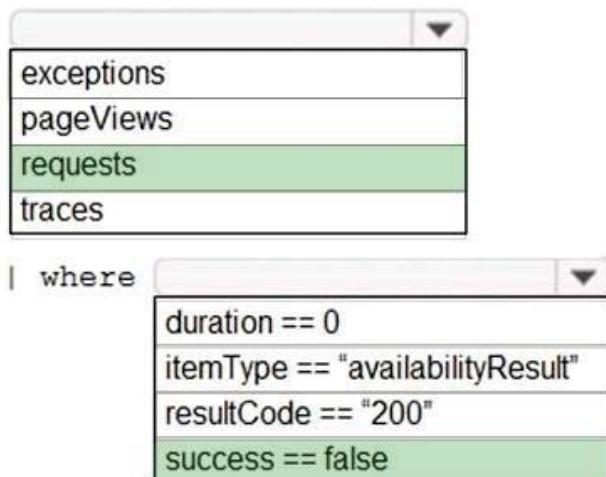
Answer Area



```
| where duration == 0
| itemType == "availabilityResult"
| resultCode == "200"
| success == false
| summarize failedCount=sum(itemCount) by name, resultCode
| top 10 by failedCount desc
| render barchart
```

Answer:

Answer Area



```
exceptions
pageViews
requests
traces

| where
    duration == 0
    itemType == "availabilityResult"
    resultCode == "200"
    success == false

| summarize failedCount=sum(itemCount) by name, resultCode
| top 10 by failedCount desc
| render barchart
```

Explanation:

Box 1: requests

Failed requests (requests/failed):

The count of tracked server requests that were marked as failed.

Kusto code:

requests

| where success == 'False'

Box 2: success == false

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/app-insights-metrics>

QUESTION 289

Hotspot Question

You have a project in Azure DevOps named Contoso App that contains pipelines in Azure Pipelines for GitHub repositories.

You need to ensure that developers receive Microsoft Teams notifications when there are failures in a pipeline of Contoso App.

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

NOTE: Each correct selection is worth one point.

Answer Area

@azure pipelines

feedback
signin
subscribe
subscriptions

https://dev.azure.com/contoso/contoso-app/
https://dev.azure.com/contoso/contoso-app/_build
https://dev.azure.com/contoso/contoso-app/_packaging
https://dev.azure.com/contoso/contoso-app/_work-items

Answer:**Answer Area**

@azure pipelines

feedback
signin
subscribe
subscriptions

https://dev.azure.com/contoso/contoso-app/
https://dev.azure.com/contoso/contoso-app/_build
https://dev.azure.com/contoso/contoso-app/_packaging
https://dev.azure.com/contoso/contoso-app/_work-items

Explanation:

Box 1: subscribe

To start monitoring all pipelines in a project, use the following command inside a channel:

@azure pipelines subscribe [project url]

Box 2: https://dev.azure.com/contoso/contoso-app/

Subscribe to a pipeline or all pipelines in a project to receive notifications:

@azure pipelines subscribe [pipeline url/ project url]