Vendor: Microsoft
Exam Code: AZ-400
Exam Name: Microsoft Azure DevOps Solutions
Version: 20.111

Q1. Case Study 1 - Litware (Q 1 - Q 5)
Overview
Existing Environment
Litware, Inc. e 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'
```

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/registerazurermautomationdscnode?view=azurermps-6.13.0

Q2. What should you use to implement the code Quality restriction on the release pipeline for the investment planning applications suite?

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

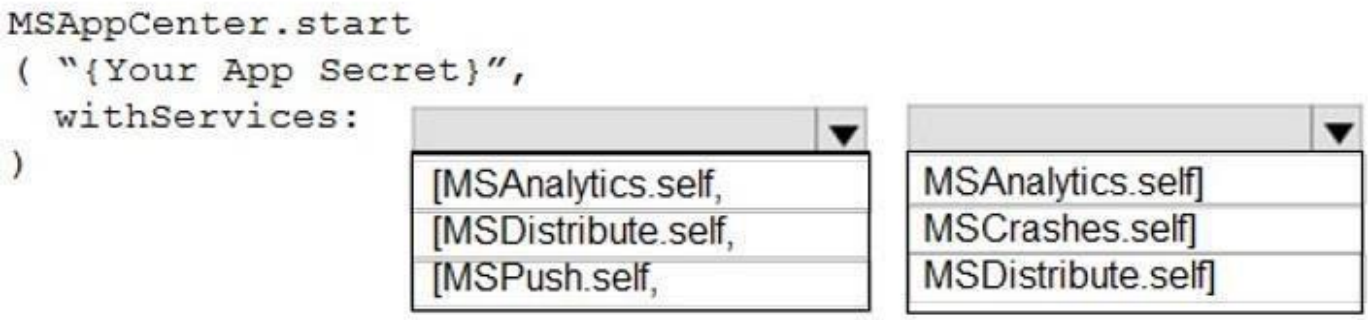
Answer: B

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

Q3.
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.

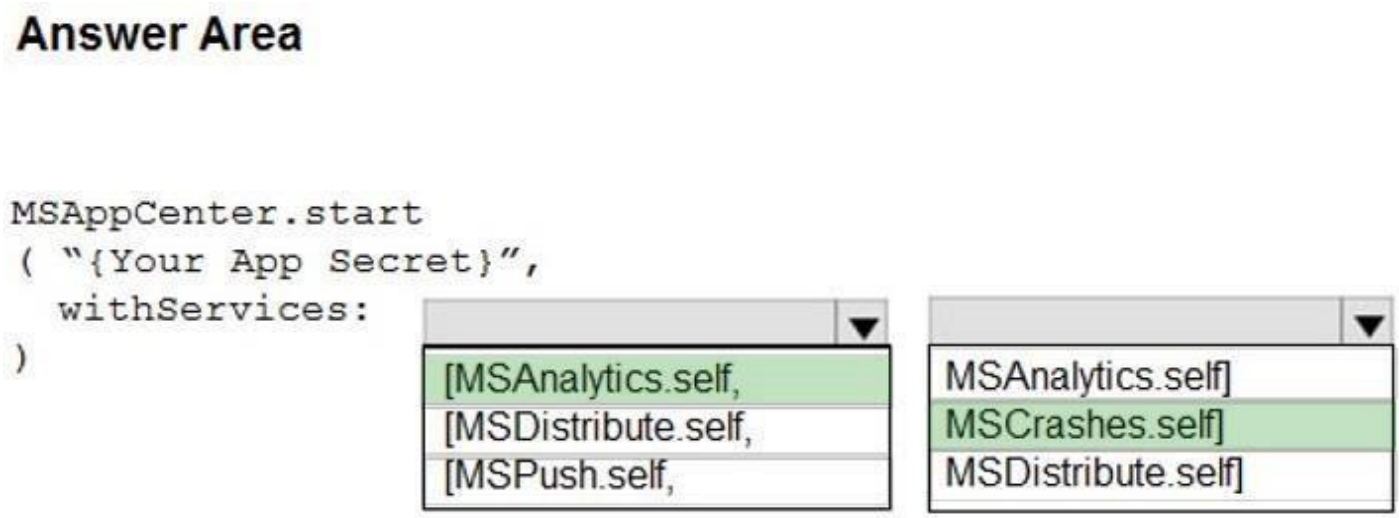
Answer Area



Box1
A. [MSAnalytics.self,
B. [MSDistribute.self],
C. [MSPush.self,
Box2
D. MSAnalytics.self]
E. MSCrashes.self]
F. MSDistribute.self]

Answer: AE

Answer Area

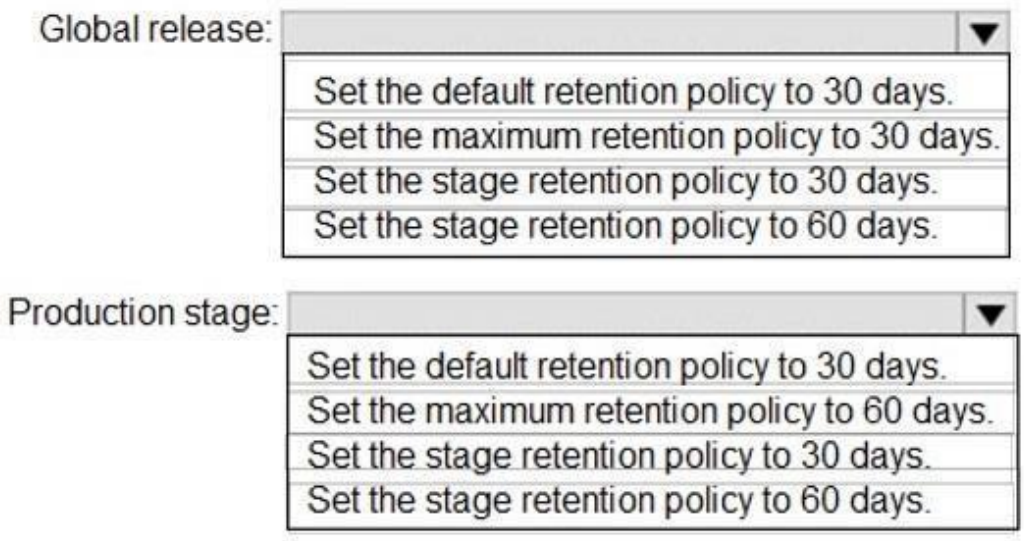


Explanation:

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

Q4. 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.

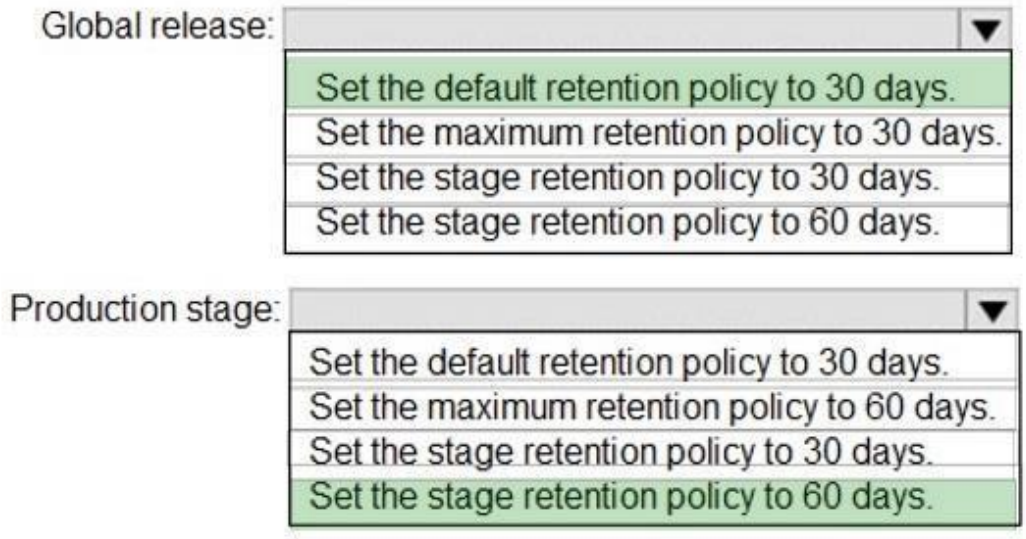
Answer Area



Box1
A. Set the default retention policy 30 days.
B. Set the maximum retention policy to 30 days.
C. Set the stage retention policy to 30 days.
D. Set the stage retention policy to 60 days.
Box2
E. Set the default retention policy 30 days.
F. Set the maximum retention policy to 60 days.
G. Set the stage retention policy to 30 days.
H. Set the stage retention policy to 60 days.

Answer: AH

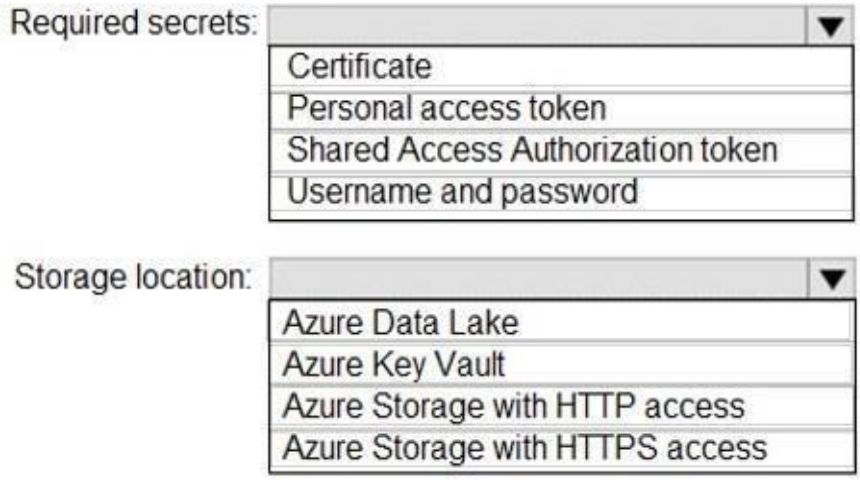
Answer Area



Explanation:
Scenario: By default, all release 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

Q5. Hotspot question
You need to configure a cloud service to store the secrets required by the mobile applications to call the share pricing service.
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.

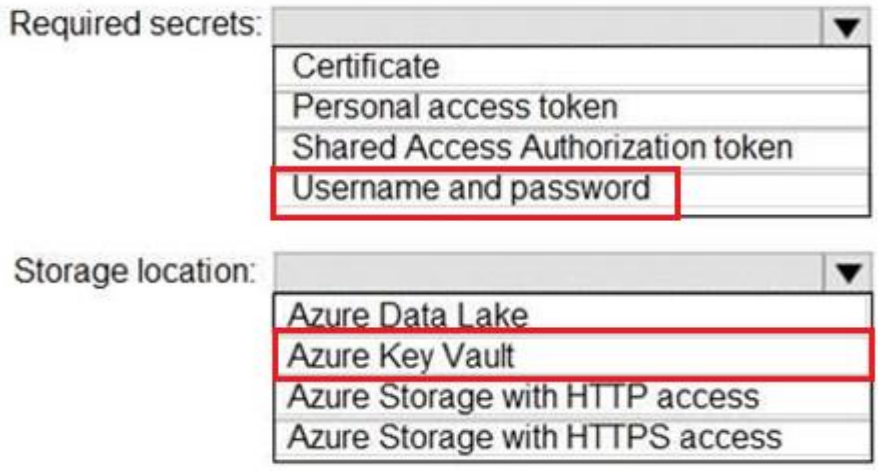
Answer Area



Box1
A. Certificate
B. Personal access token
C. Shared Access Authorization token
D. Username and password
Box2
E. Azure Data Lake
F. Azure Key Vault
G. Azure Storage with HTTP access
H. Azure Storage with HTTPS access

Answer: DF

Answer Area



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

Q6. **Case Study 2 - Contoso, Ltd (Q 6 - Q 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:
You add the virtual machines as managed nodes in Azure Automation State Configuration.
You need to configure the managed computers in Pool7.
What should you do next?

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

Answer: B

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/registerazurermautomationdscnode

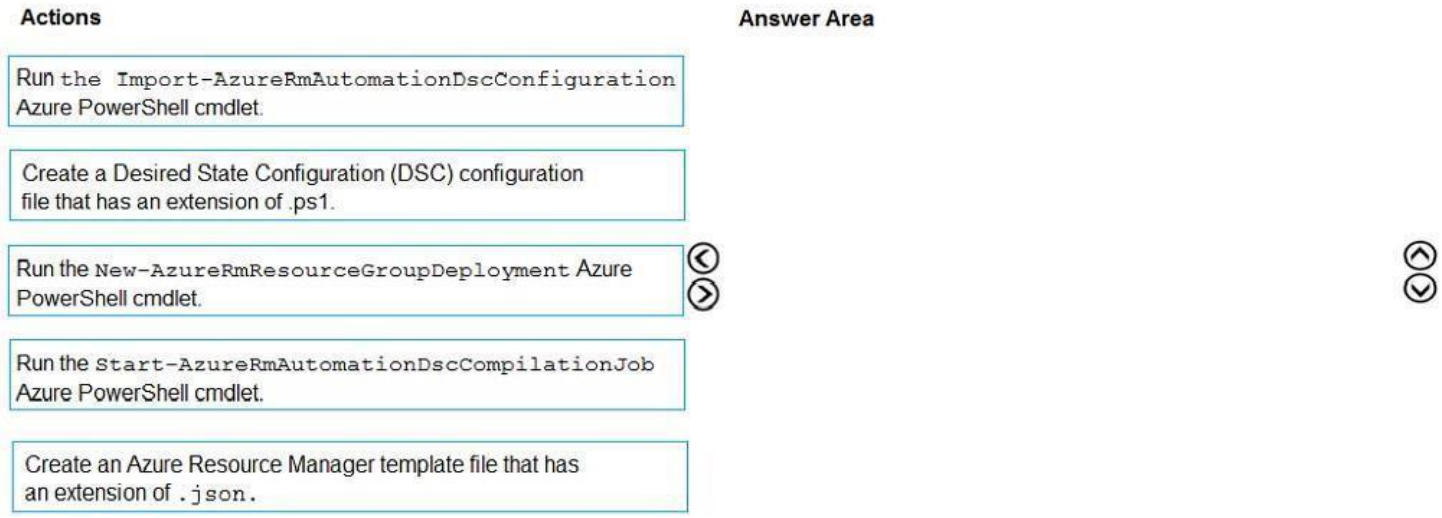
Q7. In Azure DevOps, you create Project3.
You need to meet the Requirements of the project.
What should you do first?

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: D

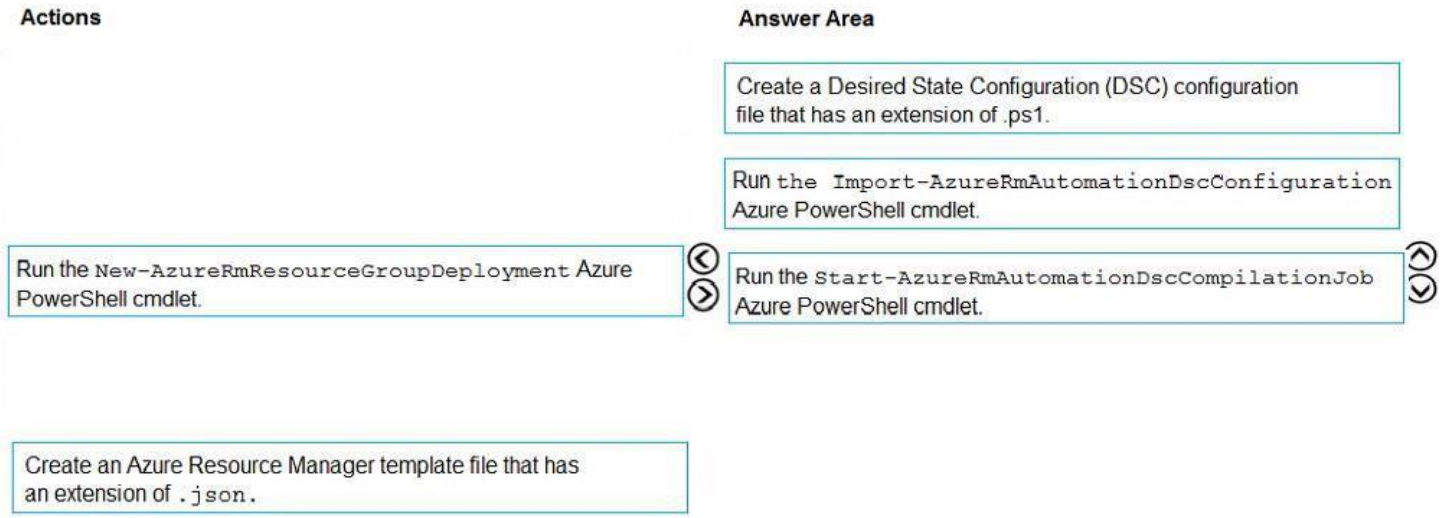
Explanation:
The first thing to do is to declare your SonarQube server as a service endpoint in your VSTS/DevOps project settings.
References:
https://docs.sonarQube.org/display/SCAN/Analyzing+with+SonarQube+Extension+for+vsts-TFS

Q8. Drag and Drop question
You need to configure Azure Automation for the computers in Pool7.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Run the Import-AzureRmAutomationDscConfiguration Azure Powershell cmdlet[2]
B. Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1[1]
C. Run the New-AzureRMResourceGroupDeployment Azure
D. Run the Start-AzureRmAutomationDscCompilationJob Azure Powershell cmdlet[3]
E. Create an Azure Resource Manager template file that has an extension of .json

Answer: BAD



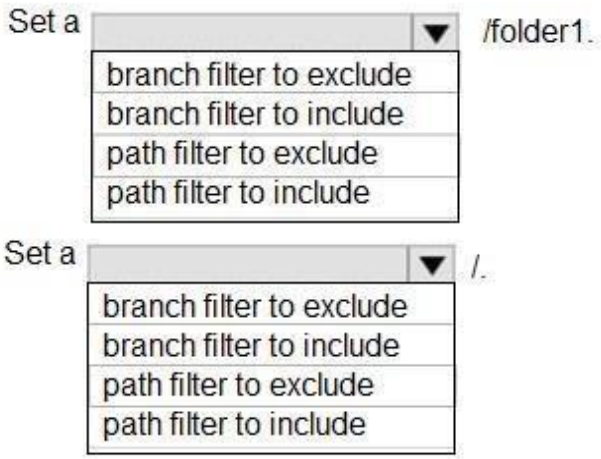
Explanation:
Step 1: Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1. Step 2: Run the Import-AzureRmAutomationDscConfiguration Azure Powershell cmdlet
The Import-AzureRmAutomationDscConfiguration cmdlet imports an APS Desired State Configuration (DSC) configuration 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/importazurermautomationdscconfiguration
https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/startazurermautomationdsccompilationjob

Q9. 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

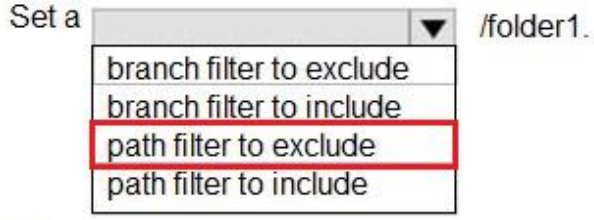


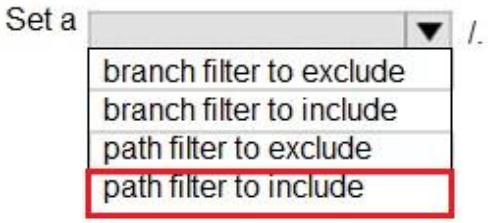
@

Box1
A. branch filter to exclude
B. branch filter to include
C. path filter to exclude
D. path filter to include
Box2
E. branch filter to exclude
F. branch filter to include
G. path filter to exclude
H. path filter to include

Answer: CH

Answer Area





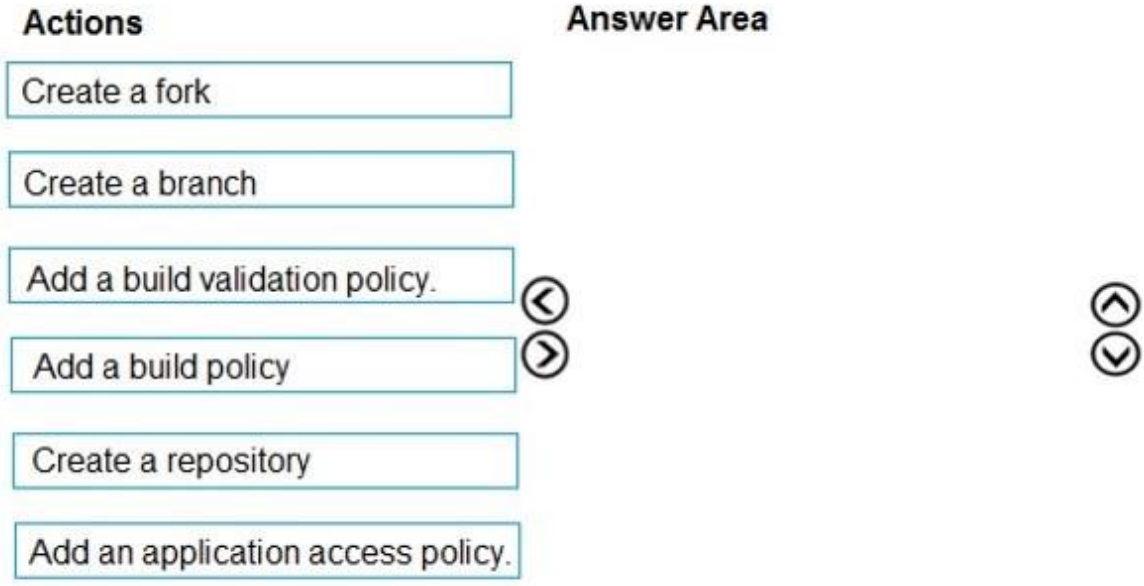
@

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

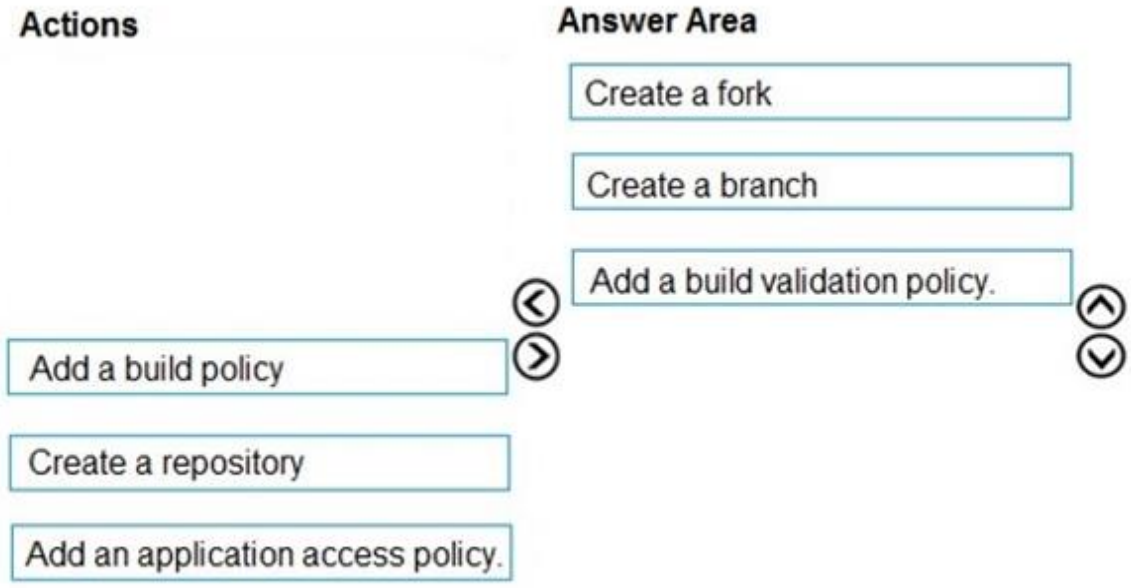
Q10. Drag and Drop question
You need to implement the code flow strategy for Project2 in Azure DevOps.
Which three actions should you perform in sequence?
To answer, move the appropriate actions from the list of actions to the answer area and arrange in the correct order.



A. Create a fork[1]
B. Create a branch[2]

C. Add a build validation policy[3]
D. Add a build policy
E. Create a repository
F. Add an application access policy

Answer: ABC



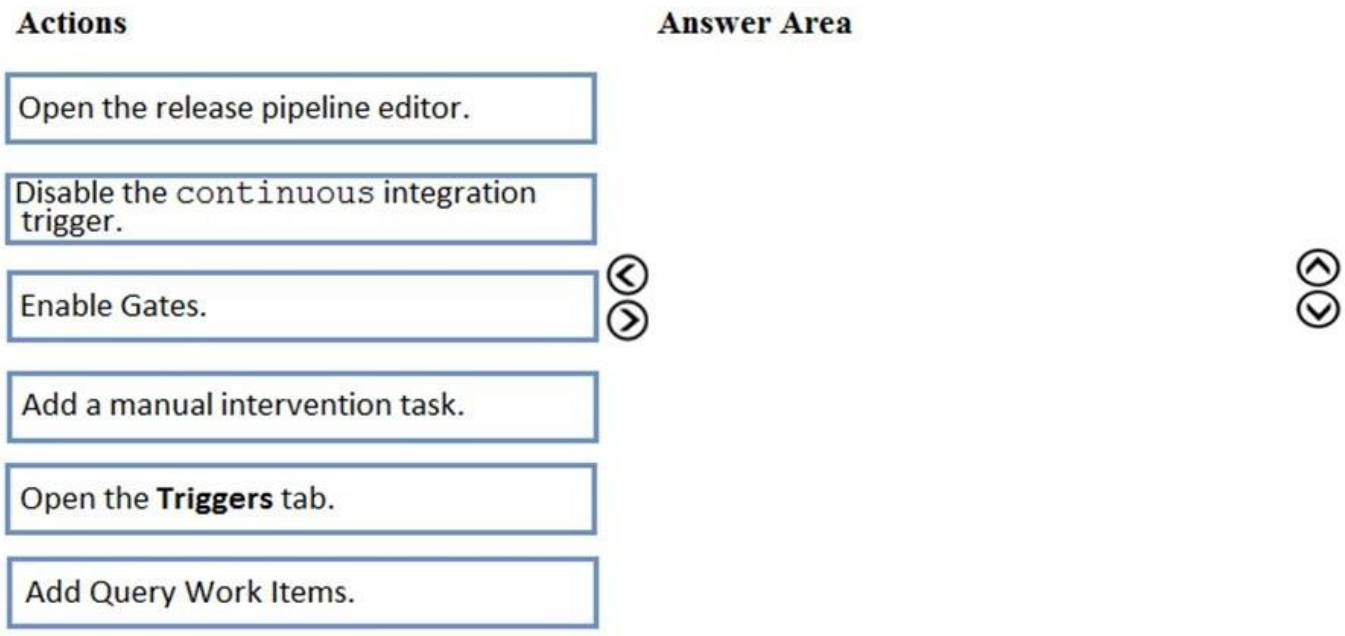
Explanation:
Step 1: Create a repository
A Git repository, or repo, is a folder that you've told Git to help you track file changes in. You can have any number of repos on your computer, each stored in their own folder.
Step 2: Create a branch
Branch policies help teams protect their important branches 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.

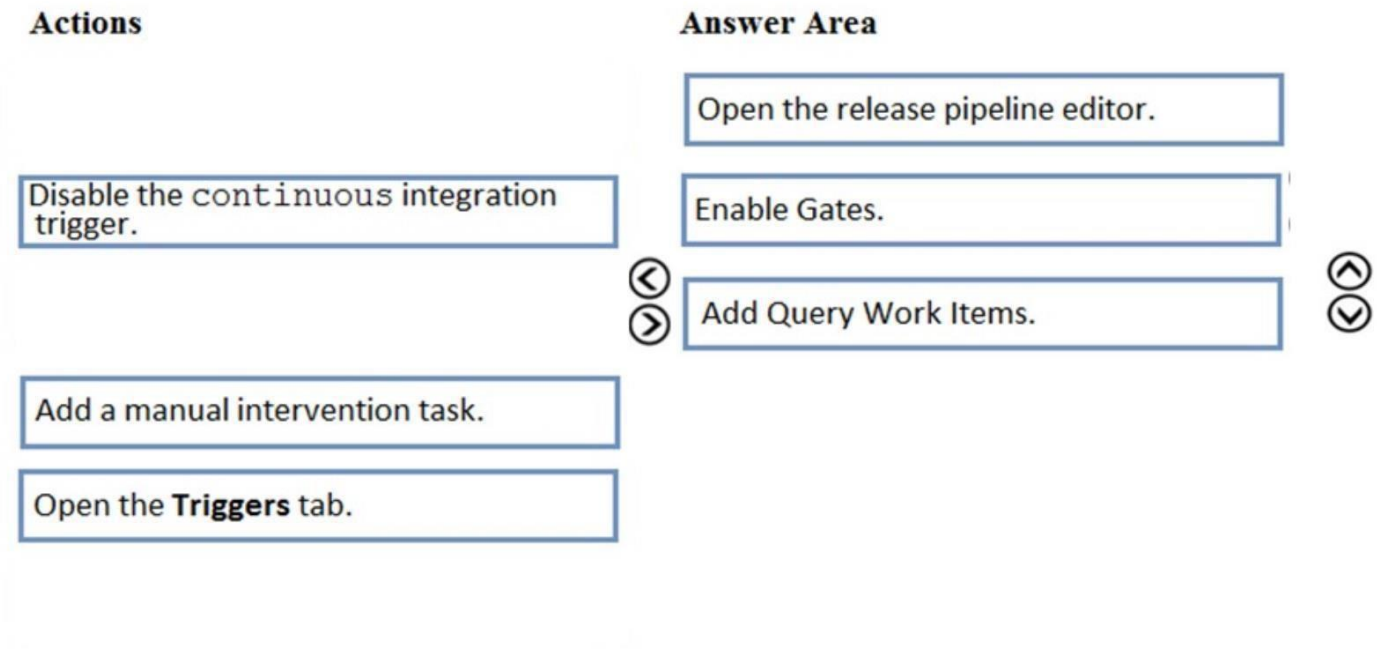
References:
https://docs.microsoft.com/en-us/azure/devops/repos/git/manage-your-branches

Q11. Drag and Drop questions
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.



A. Open the release pipeline editor[1]
B. Disable the continuous integration
C. Enable Gates[2]
D. Add manual intervention task
E. Open the Trigger tab
F. Add Query Work Items[3]

Answer: ACF



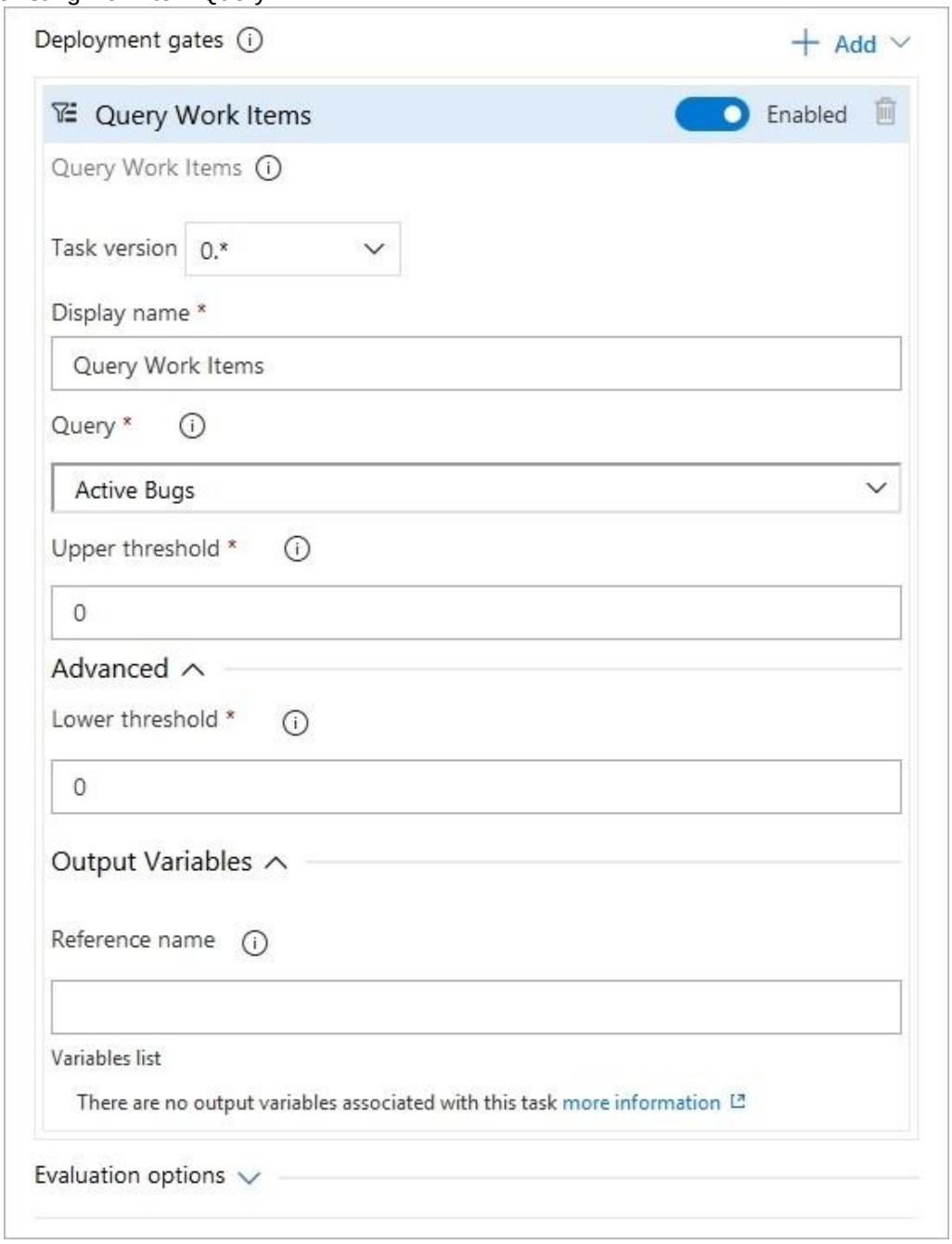
Explanation:
Scenario: Implement Project3, Project5, Project6, and Project7 based on the planned changes

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

Step 1: Open the release pipeline editor.

In the Releases tab of Azure Pipelines, select your release pipeline and choose Edit to open the pipeline editor.
Step 2: Enable Gates.
Choose the pre-deployment conditions icon for the Production stage to open the conditions panel. Enable gates by using the switch control in the Gates section. Step 3: Add Query Work items.

Choose + Add and select the Query Work Items gate.
Configure the gate by selecting an existing work item Query.



Note: A case for release gate is:
Incident and issues management. Ensure the Required status for work items, incidents, and issues. For example, ensure deployment occurs only if no priority zero bugs exist, and validation that there are no active incidents takes place after deployment.

References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deploy-usingapprovals?view=azuredevops#configure-gate

Q12. 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

Q13. 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

Q14. 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 Timeout setting for post-deployment approvals.
Does this meet the goal?

A. Yes
B. NO

Answer: B

Q15. 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

Q16. 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: A

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

Q17. 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 Enable continuous integration.
Does the meet the goal?

A. Yes
B. NO

Answer: A

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

Q18. You 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 selected Batch changes while a build is in progress
Does this meet the goal?

A. Yes
B. NO

Answer: B

Q19. Your company has a project in Azure DevOps for a new web application.
You need to ensure that when code is checked in, a build runs automatically.

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

A. Yes
B. NO

Answer: B

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

Q20. You plan to create an image that will contain a .NET Core application. You have a Dockerfile file that contains the following code. (Line numbers are included for reference only.)

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

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

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

Answer: C

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

Q21. 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. a Microsoft-hosted agent
B. Azure DevOps self-hosted agents on Azure DevTest Labs virtual machines.
C. Azure DevOps self-hosted agents on Hyper-V virtual machines
D. Azure DevOps self-hosted agents on virtual machines that run on Azure Stack

Answer: D

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

Q22. 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
E. NUnit
F. Coverage.py

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

Q23. 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. PowerShell Desired State Configuration (DSC)
C. Docker Swarm
D. single-stage builds

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/

Q24. 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*
- *Uses the custom Azure Resource Manager template to provision the virtual machines*

What should you do?

A. In Azure Cloud Shell, run Azure CLI commands to create and delete the new virtual machines in a staging resource group.

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

Answer: D

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

Q25. You manage build pipelines and deployment pipelines by using Azure DevOps.
Your company has a team of 500 developers. New members are added continual 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-basedresource-management?view=vsts&tabs=new-nav https://docs.microsoft.com/enus/rest/api/azure/devops/memberentitlementmanagement/?view=azure-devops-rest-5.0

Q26. 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 of the code.
What should you recommend?

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

Answer: B

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/

Q27. 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 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:
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 altogether. 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

Q28. 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. Configure post-deployment approvals in the deployment pipeline.
B. Configure pre-deployment approvals in the deployment pipeline.
C. Integrate Azure DevOps and SonarQube.
D. Integrate Azure DevOps and Azure DevTest Labs.

Answer: BC

Q29. 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 integration pipeline and a scheduled task that analyzes the image registry
B. manual tasks performed during the planning phase and the deployment phase
C. a task executed in the continuous deployment pipeline and a scheduled task against a running production container
D. a task executed in the continuous integration pipeline and a scheduled task that analyzes the production container

Answer: A

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-cicdpipeline?view=vsts

Q30. 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. Availability tests in Azure Application Insights
C. Profiler in Azure Application Insights
D. Application Map in Azure Application Insights

Answer: B

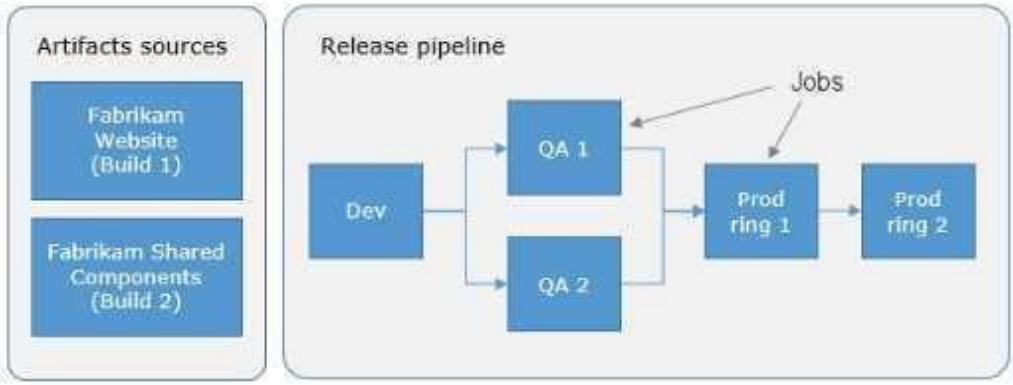
Explanation:
Application Map helps you spot performance bottlenecks or failure hotspots across all components of your distributed application. Each node on the map represents an application component or its dependencies; and has health KPI and alerts status.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-map

Q31. Your company has a project in Azure DevOps for a new web application.
The company uses ServiceNow 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 ServiceNow REST API.
B. Define a pre-deployment gate before the deployment to the Prod stage.
C. Define a deployment control that invokes the ServiceNow SOAP API.
D. Define a post-deployment gate after the deployment to the QA stage.

Answer: BD

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



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

Q32. Your company has an on-premises Bitbucket Server that is used for Git-based source control.
The server is protected by a firewall that blocks inbound Internet traffic.
You plan to use Azure DevOps to manage the build and release processes
Which two components are Required to integrate Azure DevOps and Bitbucket?
Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one port.

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

Answer: DE

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

Q33. You have a branch 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. Add the user to the Build Administrators group.
B. Add the user to the Project Administrators group.
C. From the Security settings of the repository, modify the access control for the user.
D. From the Security settings of the branch, modify the access control for the user.

Answer: D

Explanation:

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

Q34. 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. Azure Key Vault
B. a Web.config file
C. an Appsettings.json file
D. an Azure Storage table
E. an Azure Resource Manager parameter file

Answer: A

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-keyvaultparameter

Q35. Your company uses a Git repository in Azure Repos to manage the source code of a web application. The master branch is protected from direct updates.
Developers work on new features in the topic branches.
Because of the high volume of requested features, it is difficult to follow the history of the changes to the master branch.
You need to enforce a pull request merge strategy. The strategy must meet the following requirements:

- *Consolidate commit histories*
- *Merge the changes into a single commit.*

Which merge strategy should you use in the branch policy?

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

Answer: A

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

Q36. 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. Create a webhook in Jenkins.
B. Add the Team Foundation Server (TFS) plug-in to Jenkins.
C. Add a domain to your Jenkins account.
D. Create a personal access token in your Azure DevOps account.
E. Create a service hook in Azure DevOps.

Answer: BDE

Explanation:https://blogs.msdn.microsoft.com/devops/2017/04/25/vsts-visual-studio-team-servicesintegration-withjenkins/
http://www.aisoftwarellc.com/blog/post/how-to-setup-automated-builds-using-jenkins-and-visualstudio-team-foundationserver/2044

Q37. 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. OAuth
B. GitHub App
C. a personal access token
D. SAML

Answer: B

Explanation:
You can authenticate as a GitHub App.
References: https://developer.github.com/apps/building-github-apps/authenticating-with-github-apps/

Q38. You plan to share packages that you wrote, tested, validated, and deployed by using Azure Artifacts.
You need to release multiple builds of each package by using a single feed. The solution must limit the release of packages that are in development.
What should you use?

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

Answer: C

Explanation:
Upstream sources enable you to manage all of your product's dependencies in a single feed. We recommend publishing all of the packages for a given product to that product's feed, and managing that product's dependencies from remote feeds in the same feed, via upstream sources. This setup has a few benefits:
Simplicity: your NuGet.config, .npmrc, or settings.xml contains exactly one feed (your feed).
Determinism: your feed resolves package requests in order, so rebuilding the same codebase at the same commit or changeset uses the same set of packages Provenance: your feed knows the provenance of packages it saved via upstream sources, so you can verify that you're using the original package, not a custom or malicious copy published to your feed

Peace of mind: packages used via upstream sources are guaranteed to be saved in the feed on first use; if the upstream source is disabled/removed, or the remote feed goes down or deletes a package you depend on, you can continue to develop and build References:
https://docs.microsoft.com/en-us/azure/devops/artifacts/concepts/upstream-sources?view=vsts

Q39. 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. Change the feed URL of the package
B. Create a new feed for the package
C. Promote the package to a release view.
D. Publish the package to a public NuGet repository.

Answer: B

Explanation:
Azure Artifacts introduces the concept of multiple feeds that you can use to organize and control access to your packages.
Packages you host in Azure Artifacts are stored in a feed. Setting permissions on the feed allows you to share your packages with as many or as few people as your scenario Requires. Feeds have four levels of access: Owners, Contributors, Collaborators, and Readers.
References:
https://docs.microsoft.com/en-us/azure/devops/artifacts/feeds/feedpermissions?view=vsts&tabs=new-nav

Q40. 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. Code Style
C. Black Duck
D. Jenkins
E. SourceGea
F. OWASP ZAP

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

Q41. 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. Add a devDependencies section to Package-lock.json.
C. Configure the Artifactory plug-in.
D. Delete Package-lock.json.

Answer: B

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: Shttps://blogs.msdn.microsoft.com/visualstudioalmrangers/2017/06/08/manage-your-open-sourceusage-and-security-ashttps://blogs.msdn.microsoft.com/visualstudioalmrangers/2017/06/08/manage-your-open-sourceusage-and-security-as-reported-by-your-cicd-pipeline/reported-by-your-cicd-pipeline/

Q42. 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. Azure Log Analytics
B. PL/pgSQL
C. PL/SQL
D. Transact-SQL

Answer: A

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

Q43. Your company uses Service Now for incident management.
You develop an application that runs on Azure.
The company needs to generate a ticket in ServiceNow when the application fails to authenticate.

Which Azure Log Analytics solution should you use?

A. Application Insights Connector
B. Automation & Control
C. IT Service Management Connector (ITSM)
D. Insight & Analytics

Answer: C

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

Q44. You have multi-tier application that has an Azure Web Apps front end and an Azure SQL Datable 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 Event Hubs
B. Azure SQL Database Intelligent Insights
C. Azure Application Insights
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

Q45. 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. Azure Logic Apps
B. Azure Pipelines
C. Microsoft Visual Studio App Center
D. Azure DevOps Project
E. Azure Application Insights

Answer: AE

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

Q46. 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

Suggested Answer: D
☞ 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.
Note: Slack would also be a correct answer, but it is not an option here.
References:https://searchunifiedcommunications.techtarget.com/definition/Microsoft-Teams

Q47. 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

Q48. 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

Q49. You have an approval process that contains a condition. The condition requires that releases be approved by a team leader before they are deployed.
You have a policy stating that approvals must occur within eight hours. You discover that deployment fail if the approvals take longer than two hours.
You need to ensure that the deployments only fail if the approvals take longer than eight hours.

Solution: From Pre-deployment conditions, you modify the Time between re-evaluation of gates option.
Does this meet the goal?

A. Yes
B. No

Answer: B

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.

Q50. You plan to create a release pipeline that will deploy Azure resources by using Azure Resource Manager templates. The release pipeline will create the following resources:

- *Two resource groups*
- *Four Azure virtual machines in one resource group*
- *Two Azure SQL databases in other resource group*

You need to recommend a solution to deploy the resources.
Solution: Create two standalone templates, each of which will deploy the resources in its respective group.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Use a main template and two linked templates.
References:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-linked-templates

Q51. 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

Q52. 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

Q53. 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

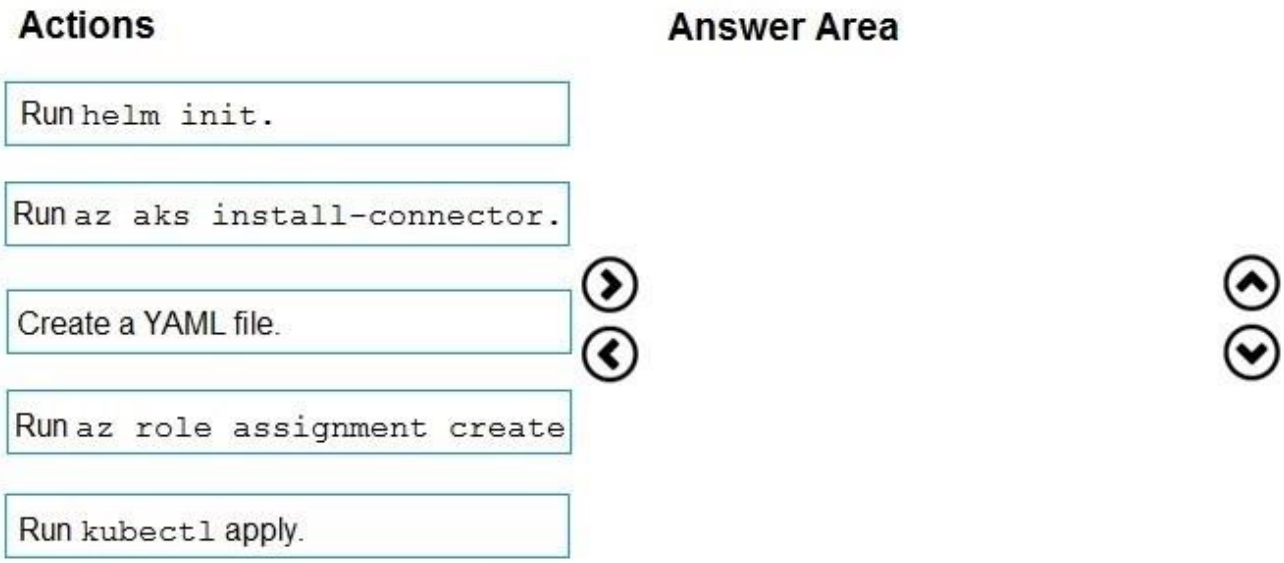
Explanation:
WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the 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/

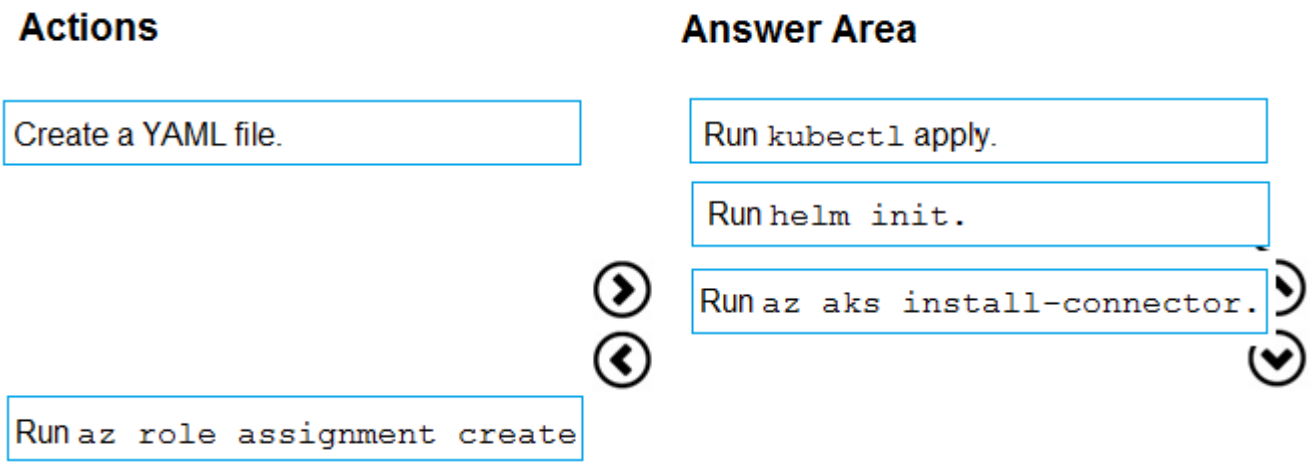
Q54. Drag and Drop question
You have an Azure Kubernetes Service (AKS) implementation that is RBAC-enabled.
You plan to use Azure Container Instances as a hosted development environment to run containers in the AKS implementation.
You need to configure Azure Container Instances as a hosted environment for running the containers in AKS.

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



A. Run helm init[2]
B. Run az aks install-connector[3]
C. Create a YAML file
D. Run az role assignment create
E. Run kubectl apply[1]

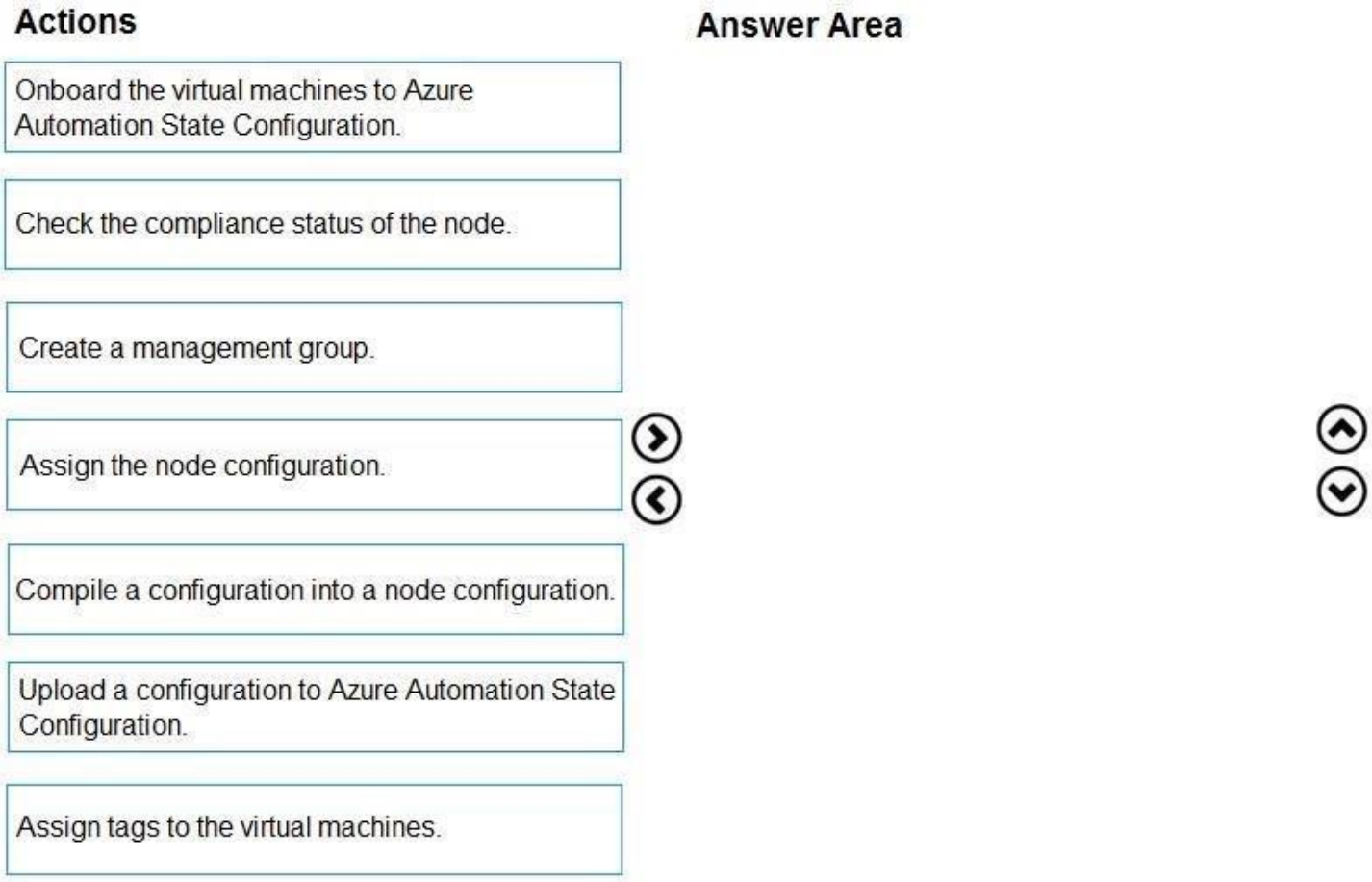
Answer: EAB



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-virtualkubelet. yaml Step 2: Run kubectl apply.
Apply the service account and binding with kubectl apply and specify your rbac-virtualkubelet.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

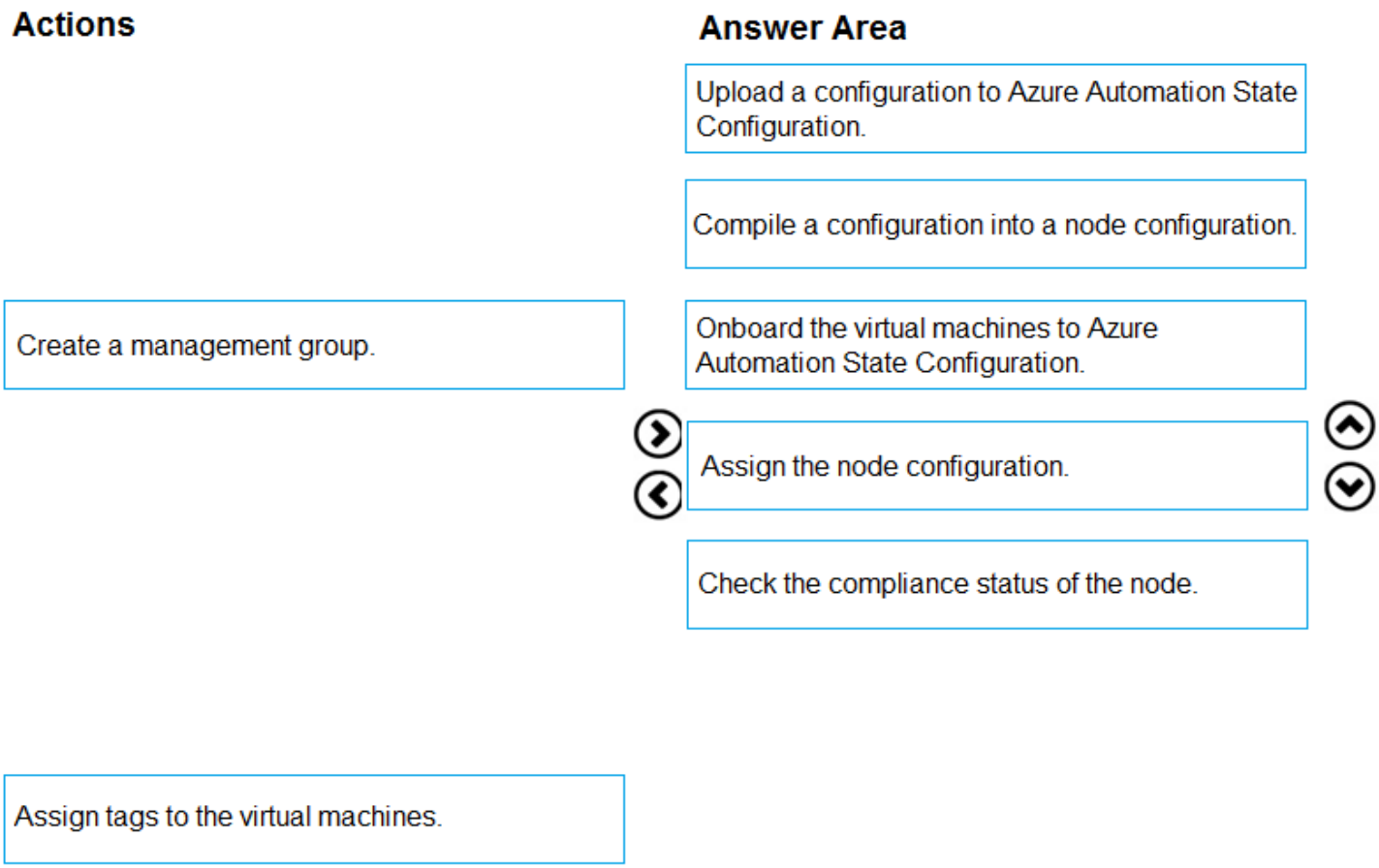
Q55. Drag and Drop question
You need to use Azure Automation State Configuration to manage the ongoing consistency of virtual machine configurations.
Which five actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



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

A. Onboard the virtual machines to Azure Automation State Configuration[3]
B. Check the compliances status of the node[5]
C. Create a management group
D. Assign the node configuration[4]
E. Compile a configuration into a node configuration[2]
F. Upload a configuration to Azure Automation State Configuration[1]
G. Assign tags to the virtual machines

Answer: FEADB

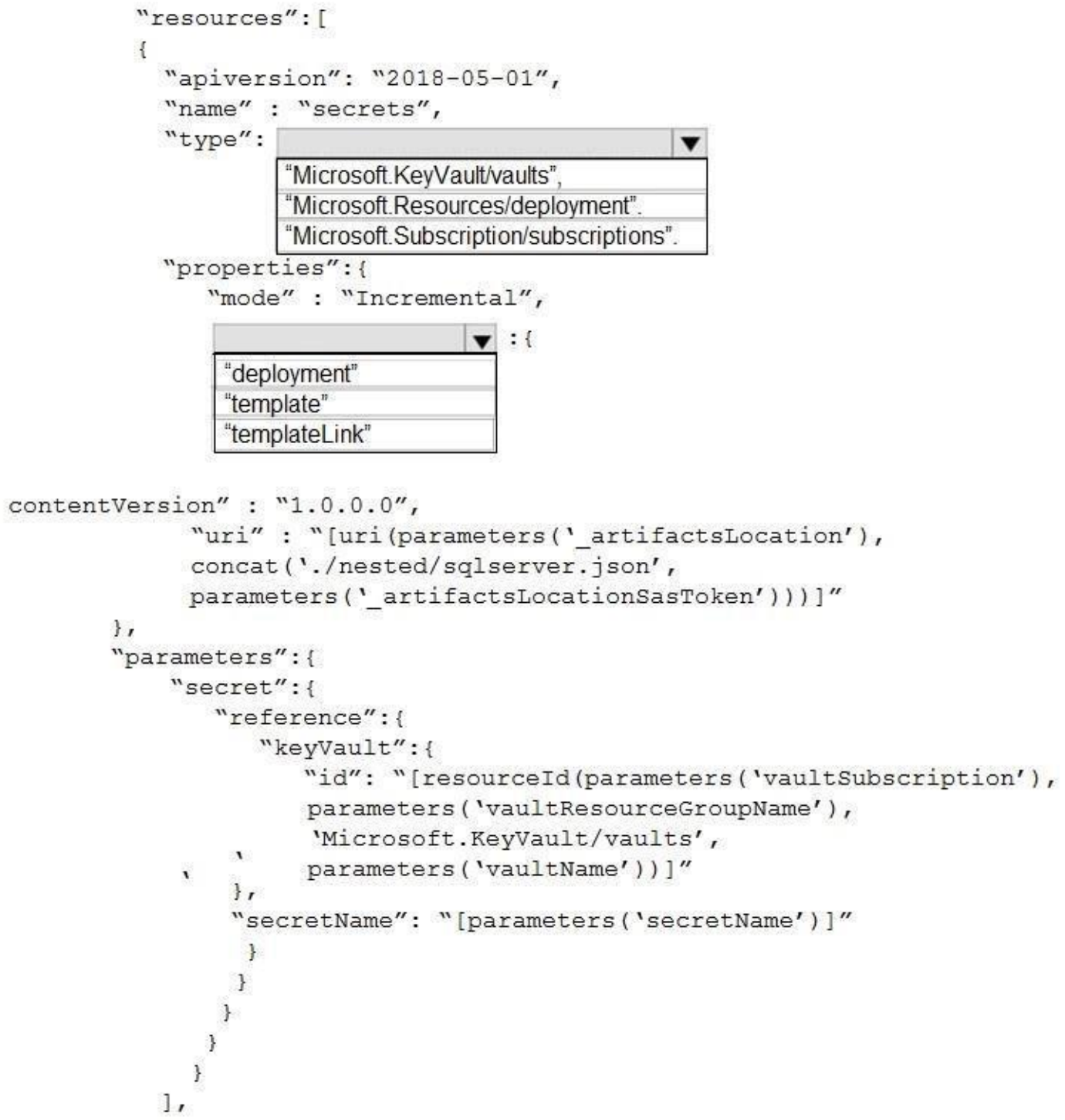


Explanation:
Step 1: Assign the node configuration.
You create a simple DSC configuration that ensures either the presence or absence of the Web-Server Windows Feature (IIS), depending on how you assign nodes. Step 2: Upload a configuration to Azure Automation State Configuration.

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

Q56. 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 eh appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Box1
A. "Microsoft.KeyVault/vaults",
B. "Microsoft.Resources/deployment",

C. “Microsoft.Subscription/subscription”,
Box2
D. “deployment”
E. “template”
F. “templateLink”

Answer: BF

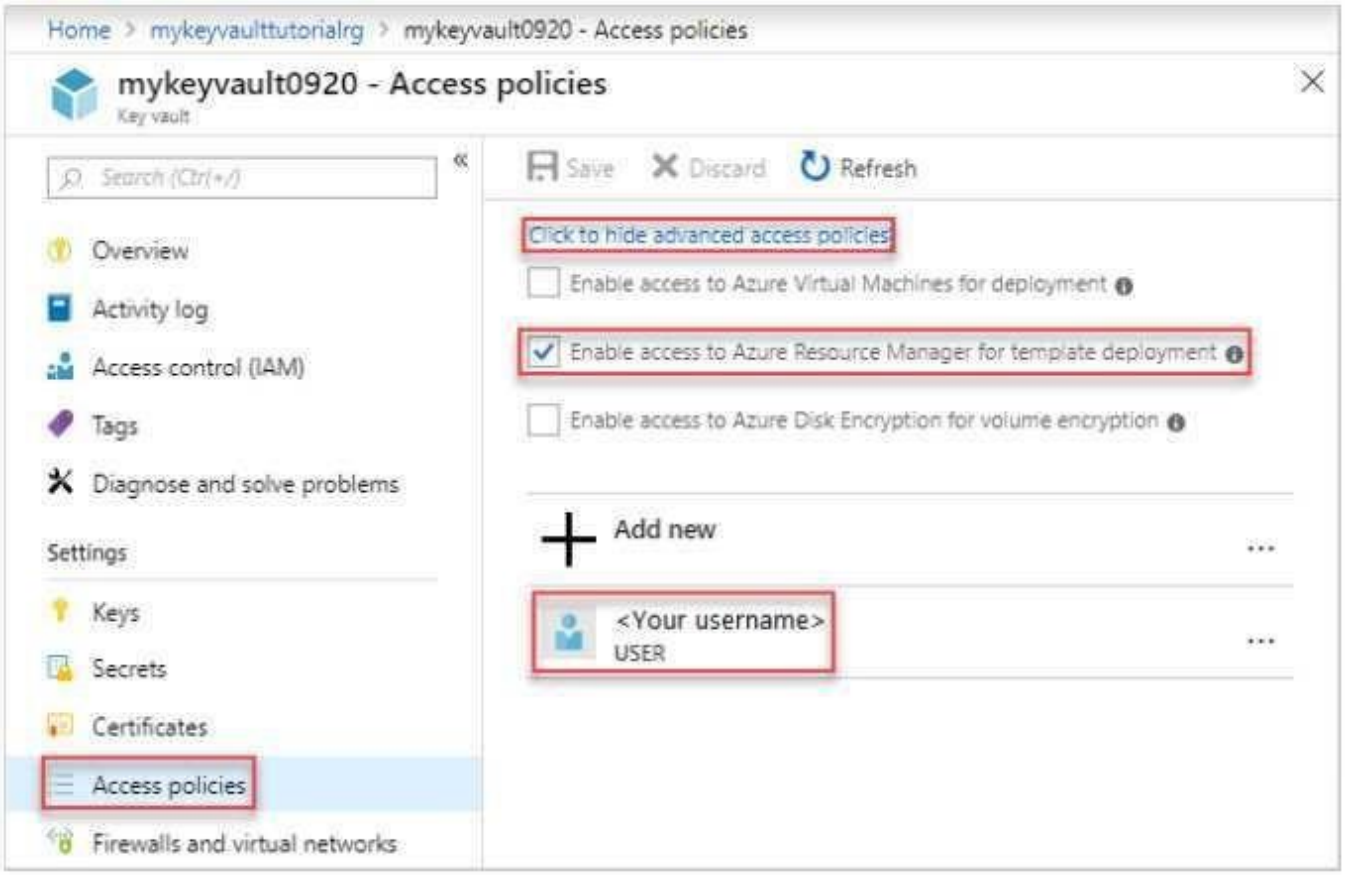
Q57. Drag and Drop question

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.

A. A Key Vault access policy(twice)
B. A Key Vault advanced access policy
C. RBAC

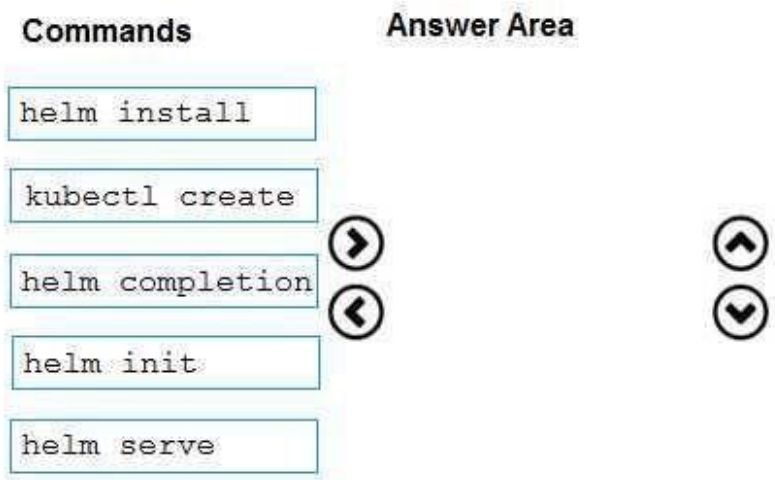
Answer: AA

Explanation:
Box 1: A key Vault advanced access policy



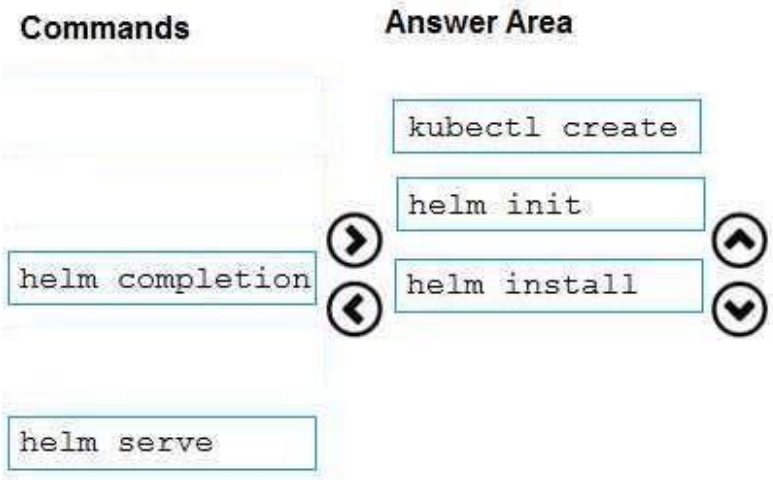
Box 2: RBAC
Management plane access control uses RBAC.
The management plane consists of operations that affect the key vault itself, such as:
Creating or deleting a key vault.
Getting a list of vaults in a subscription.
Retrieving Key Vault properties (such as SKU and tags).
Setting Key Vault access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

Q58. Drag and Drop question
You need to recommend a solution for deploying charts by using Helm and Tiller to Azure Kubernetes Service (AKS) in an RBAC-enabled cluster.
Which three commands should you recommend be run m sequence?
To answer, move the appropriate commands from the list of commands to the answer area and arrange them in the correct order.



A. helm install[3]
B. kubectl create[1]
C. helm completion
D. helm init[2]
E. helm serve

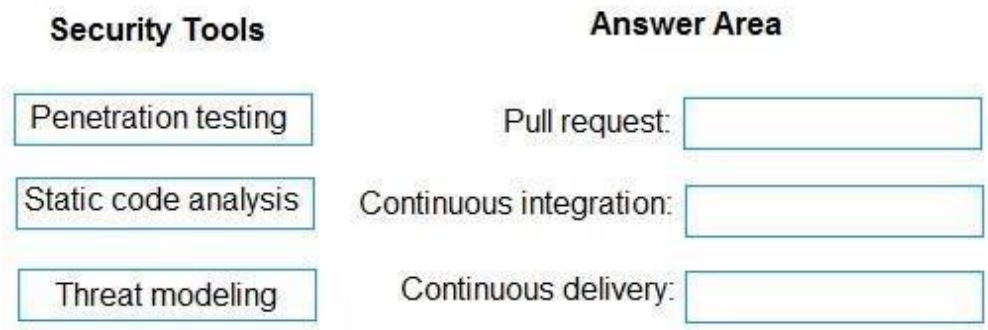
Answer: BDA



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

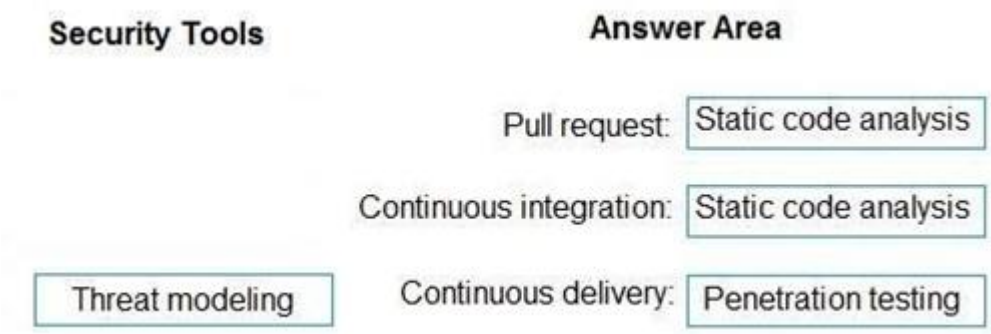
Q59. Drag and Drop question

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 toots to the correct stages.
Each security tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content
NOTE: Each correct selection is worth one point.



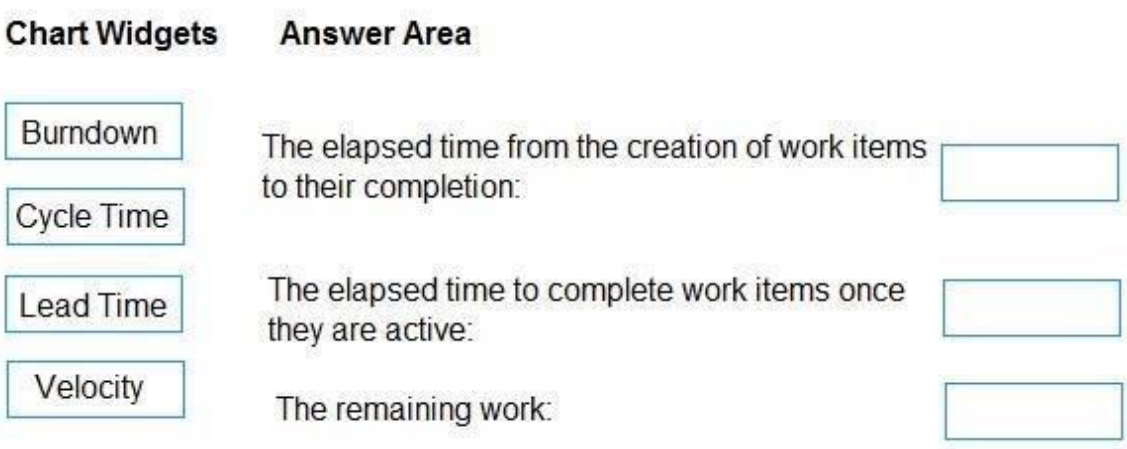
A. Penetration testing[3]
B. Static code analysis[1&2]
C. Threat modeling

Answer: BA



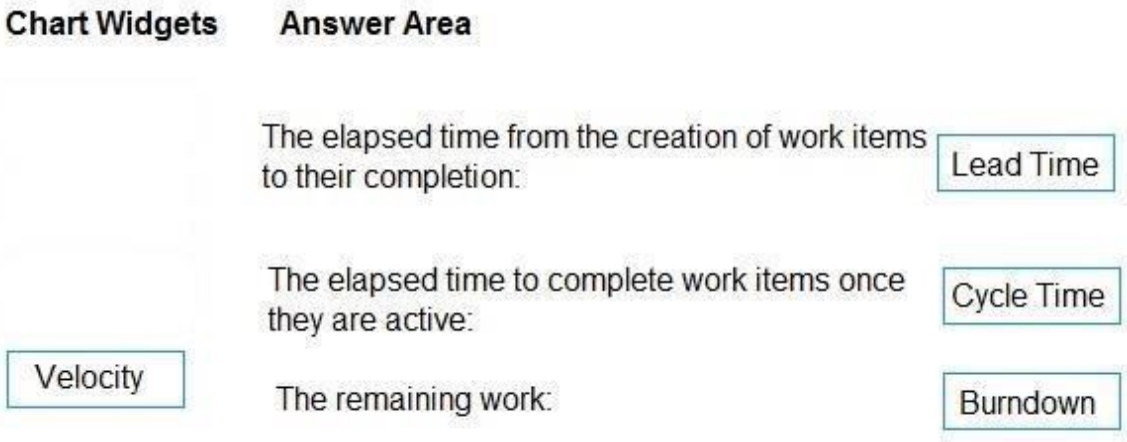
Explanation:
Box 1: Threat modeling
Threat modeling's motto should be, "The earlier the better, but not too late and never ignore." Box 2: Static code analysis
Validation in the CI/CD begins before the developer commits his or her code. Static code analysis tools in the IDE provide the first line of 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-cicdpipeline? view=vsts

Q60. 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.



A. Burndown[3]
B. Cycle Time[2]
C. Lead Time[1]
D. Velocity

Answer: CBA



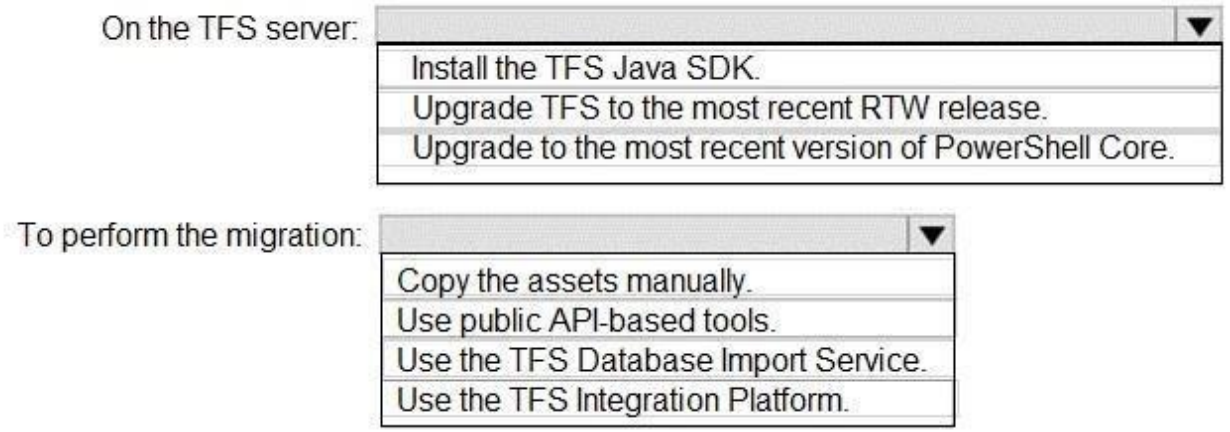
Explanation:
Box 1: Lead time
Lead time measures the total time elapsed from the creation of work items to their completion.
Box 2: Cycle time
Cycle time measures the time it takes for your team to complete work items once they begin actively working on them.
Box 3: Burndown
Burndown charts focus on 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-leadtime?view=vsts
https://docs.microsoft.com/en-us/azure/devops/report/dashboards/configure-burndown-burnupwidgets?view=vsts Q61.

Q61. 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:

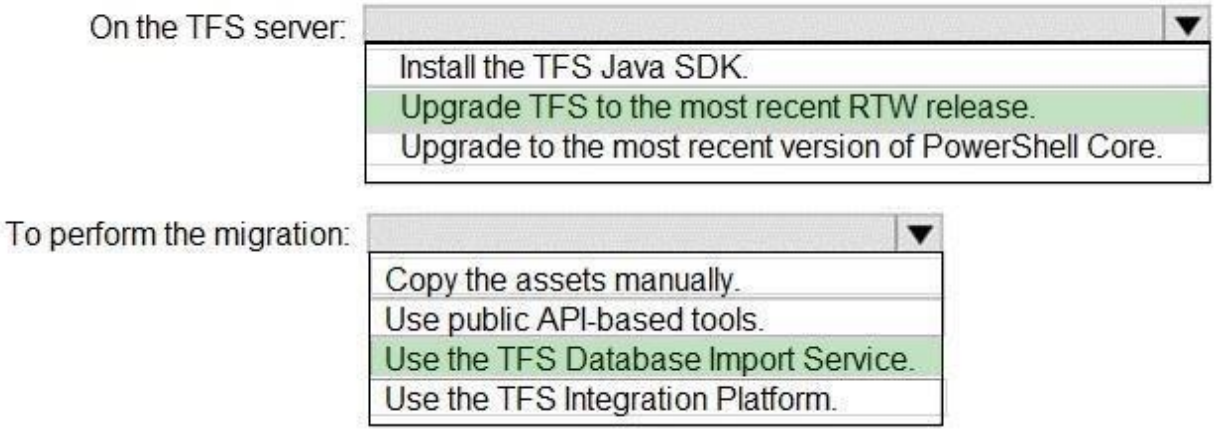
- *Preserves the dates of Team Foundation Version Control changesets*
- *Preserves the changes dates of work items revisions*
- *Minimizes migration effort*
- *Migrates all TFS artifacts*

What should you recommend?
To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Box1
A. Install the TFS Java SDK
B. Upgrade TFS to the most recent RTW release
C. Upgrade to the most recent version of the PowerShell Core
Box2
D. Copy the assets manually
E. Use public API-based tools
F. Use TFS Database Import Service
G. Use the TFS Integration Platform

Answer: BF



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

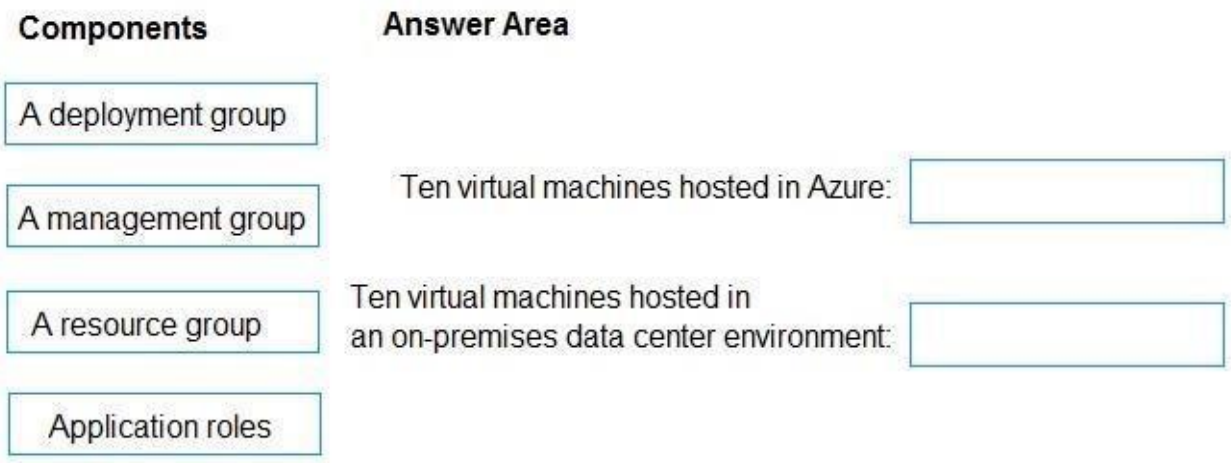
In Phase 3 of your migration project, you will work on upgrading your Team Foundation Server to one of the supported versions for the Database Import Service in Azure Devops Services. References:
Team Foundation Server to Azure Devops Services Migration Guide

Q62. 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*

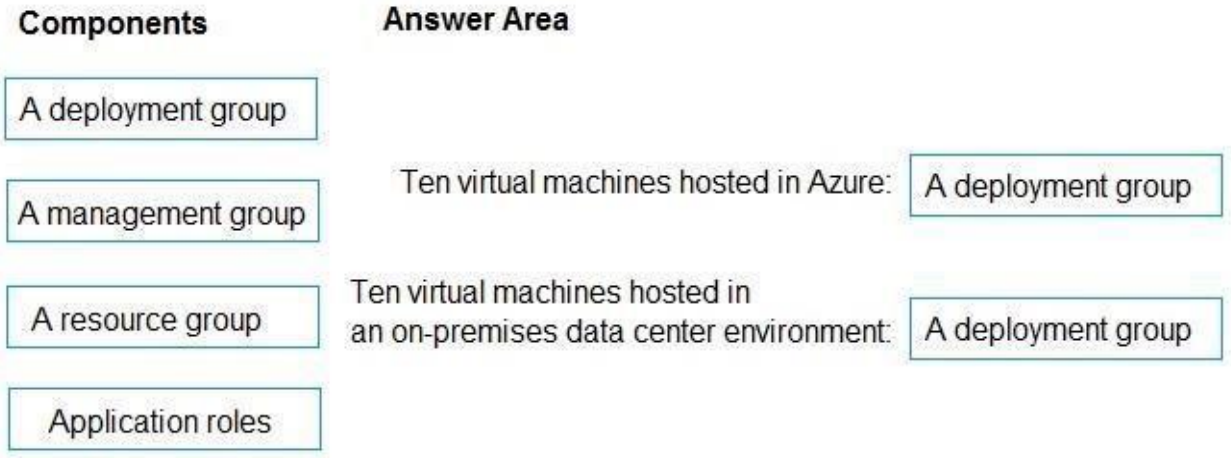
All the virtual machines have the-Azure Pipelines agent.
You need to implement a release strategy for deploying the application to the endpoints.

What should you recommend using to deploy the application to the endpoints? To answer, drag the appropriate components to the correct endpoints.
Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or soon to view content.
NOTE: Each correct selection n worth one point.



A. A deployment group (both boxes)
B. A management group
C. A resource group
D. Application roles

Answer: A



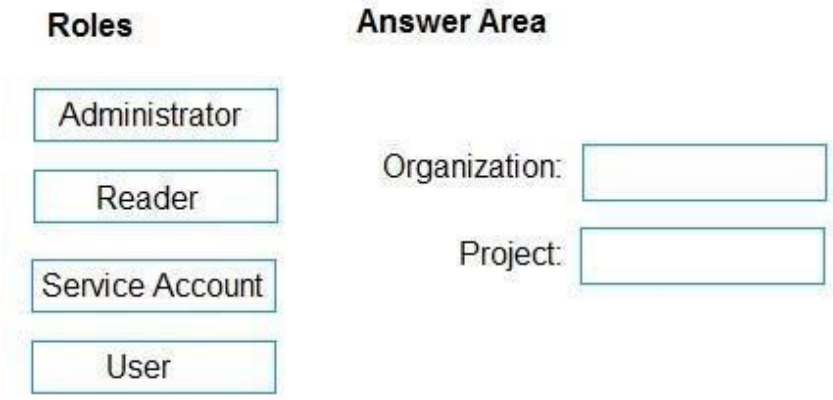
Explanation:
Box 1: A deployment group

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

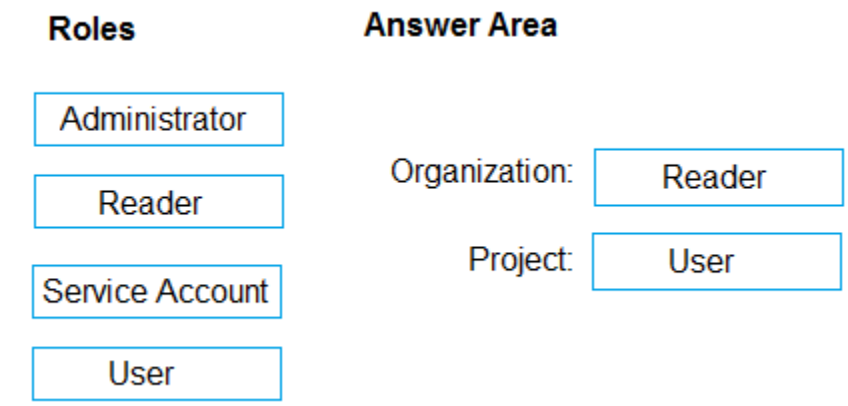
Q63. Drag and Drop question
You need to configure access to Azure DevOps Agent pools to meet the forwarding Requirements:

- *Use a project agent pool when authoring build release pipelines.*
- *View the agent pool and agents of the organization.*
- *Use the principle of least privilege.*

Which role memberships are required for the Azure 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.



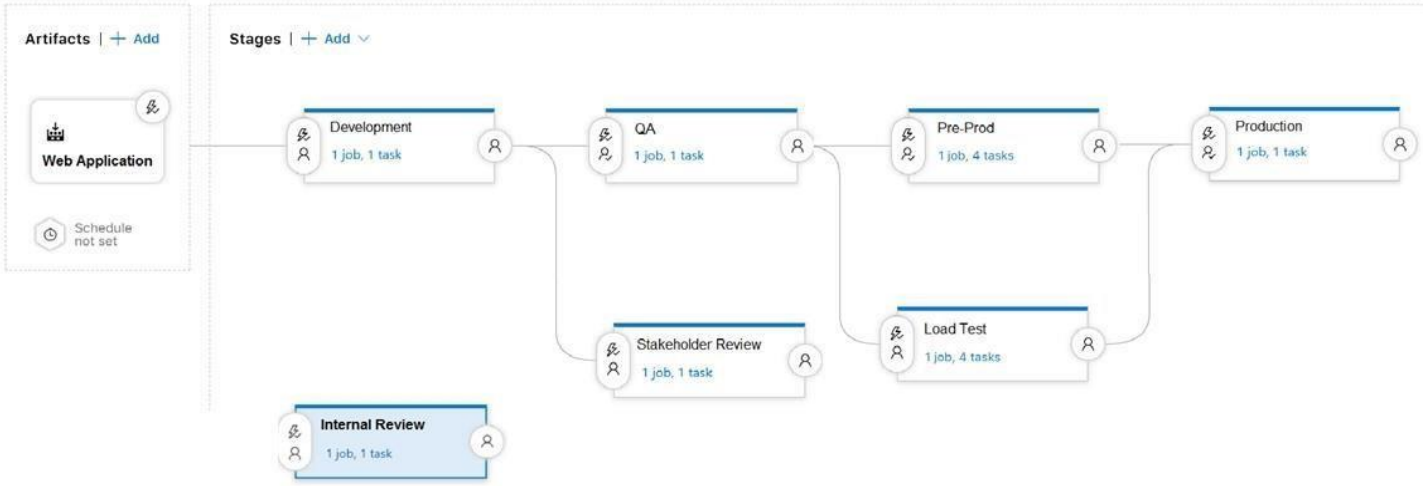
A. Administrator
B. Reader
C. Service Account
D. User
Answer: BD



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

Q64. 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

Box1
A. 0
B. 1
C. 2
D. 3
E. 4

F. 5
G. 6
H. 7
Box2
I. The Development stage
J. The Internal Review stage
K. The Production stage
L. The Web Application artifact

Answer: FJ

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

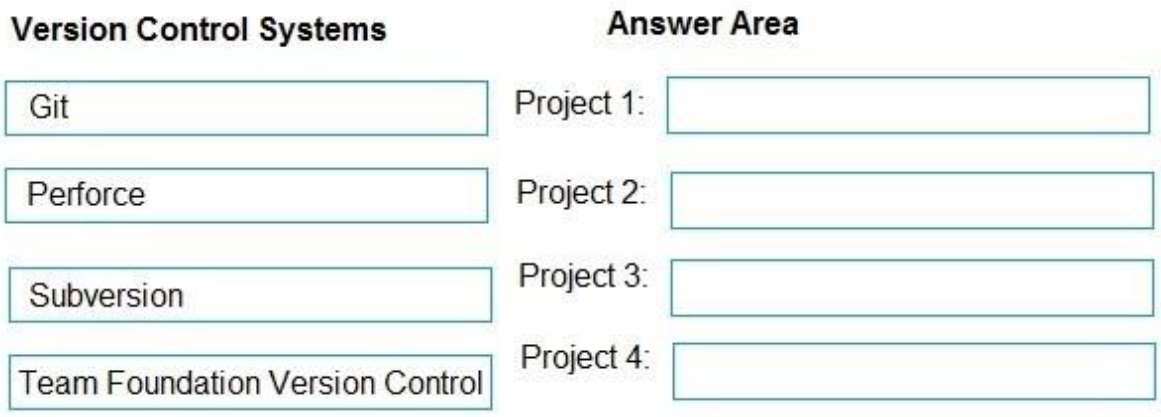
Explanation:
Box 1: 5
There are five stages: Development, QA, Pre-production, Load Test and Production. They all have triggers. Box 2: The Internal Review stage.
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/triggers

Q65. 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: • 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.

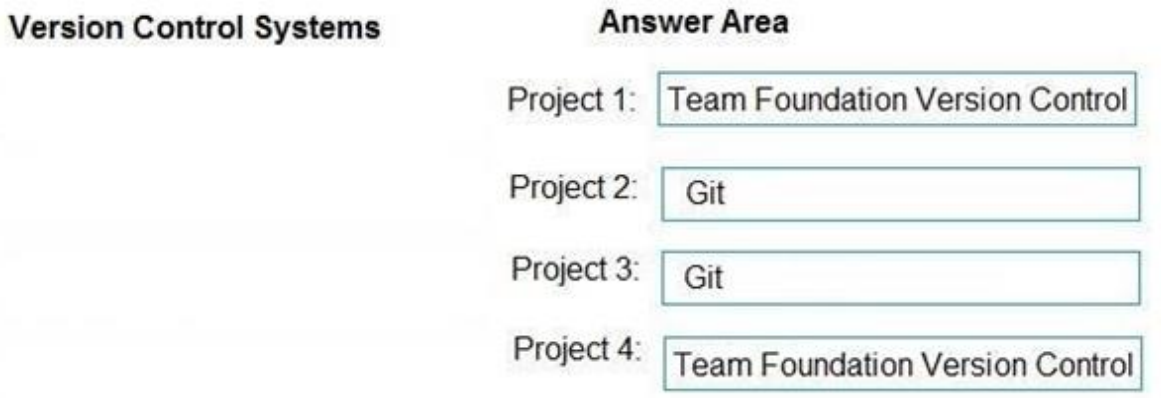
You plan to use Azure Repos for all the projects.
Which version control system should you use for each project? To answer, drag the appropriate version control systems to the correct projects.

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.



A. Git[2/3]
B. Perforce
C. Subversion
D. Team Foundation Version Control[1/4]

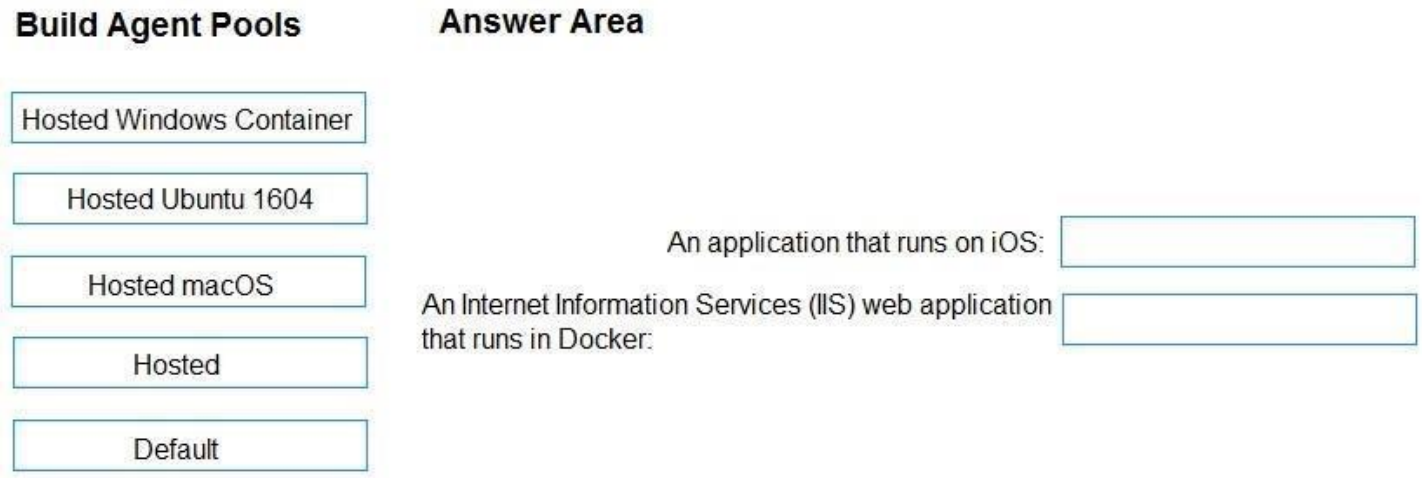
Answer: DAAD



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:

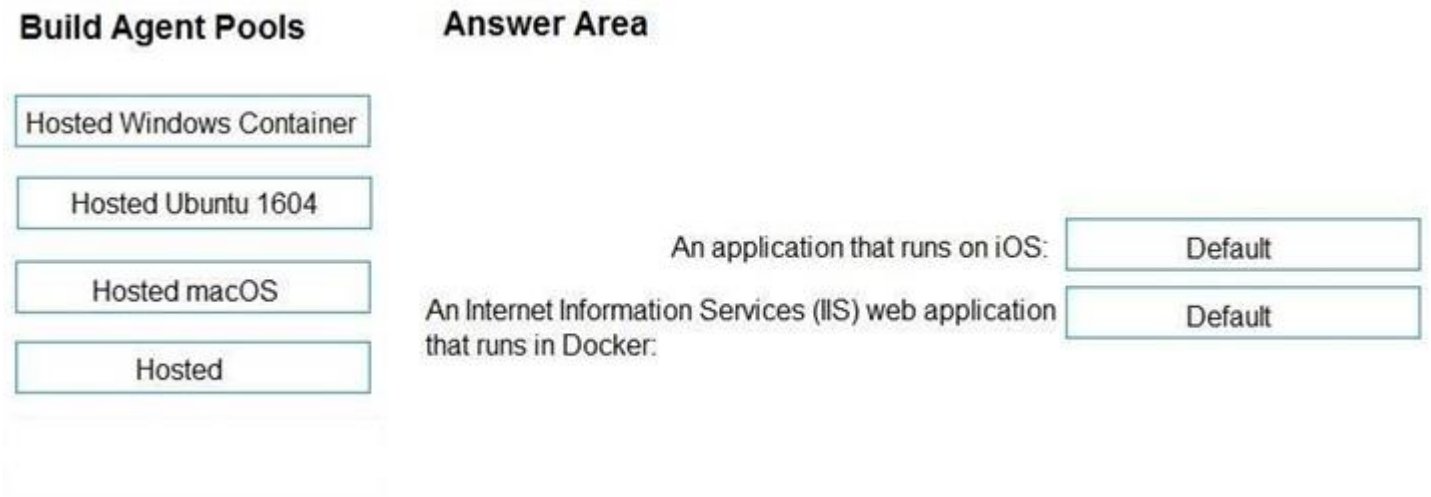
https://searchitoperations.techtarget.com/definition/Perforce-Software
https://docs.microsoft.com/en-us/azure/devops/repos/git/share-your-code-in-git-xcode https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/overview

Q66. 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 build 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.



A. Hosted Windows Container
B. Hosted Ubuntu 1604
C. Hosted macOS
D. Hosted
E. Default (twice)

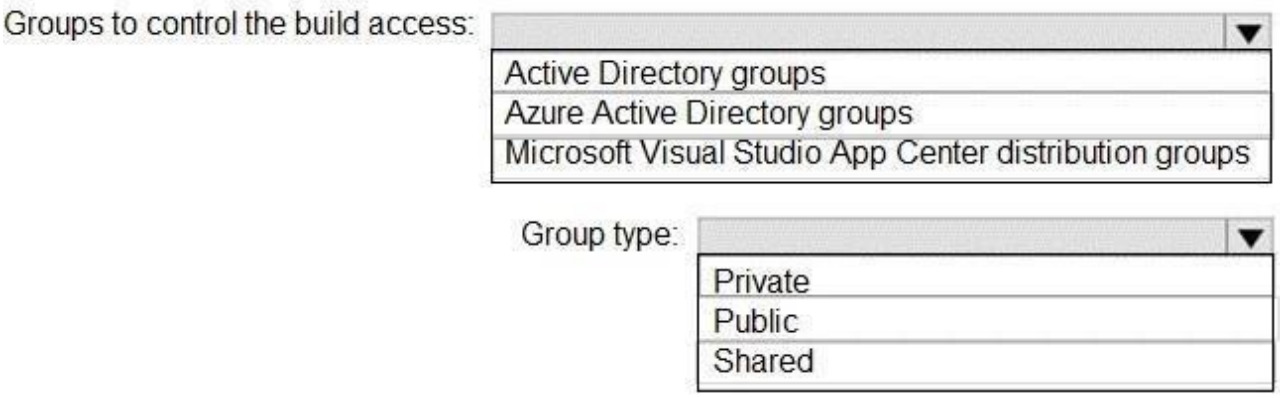
Answer: E



Explanation:
Box 1: Default

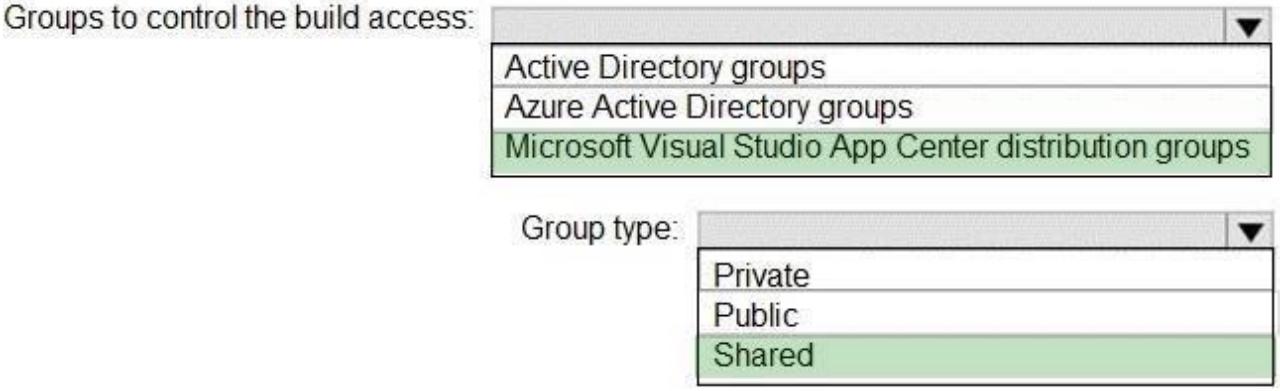
Box 2: Default

Q67. 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.



Box1
A. Active Directory groups
B. Azure Active Directory groups
C. Microsoft Visual Studio App Center distribution groups
Box2
D. Private
E. Public
F. Shared

Answer: CF



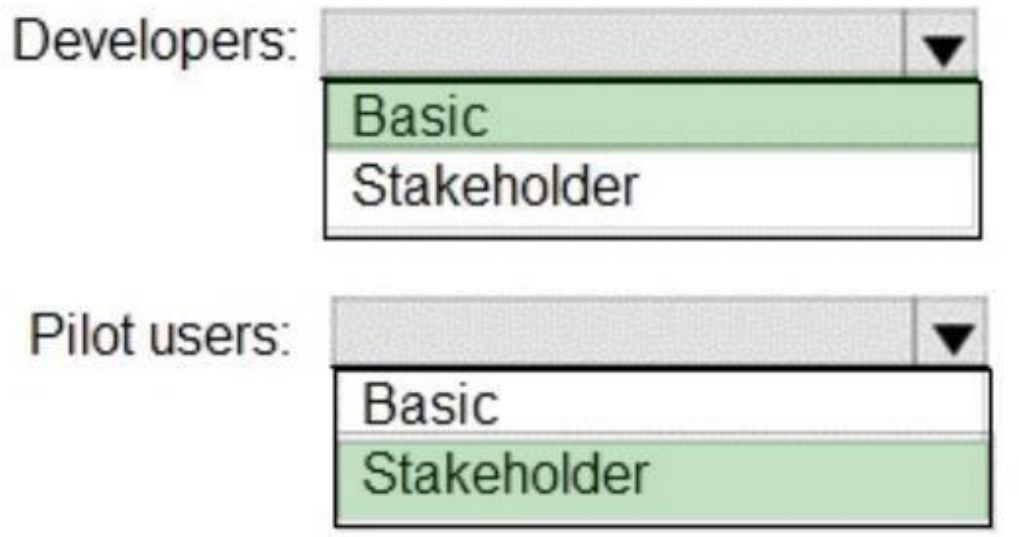
Explanation:
Box 1: Microsoft Visual Studio App Center distribution Groups Distribution Groups are used to control access to releases. A Distribution Group represents a set of users that can be managed jointly and can have common access to releases. Example of Distribution Groups can be teams of users, 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

Q68. 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 m Azure DevOps should you identify? To answer, select the appropriate options in the answer area
NOTE: Each correct selection is worth one point.

Box1
A. Basic
B. Stakeholder
Box2
C. Basic
D. Stakeholder

Answer: AD



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

Q69. 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

Q70. Your company develops an app for OS. All users of the app have devices that are members of a private distribution group in Microsoft Visual Studio App Center. You plan to distribute a new release of the app.
You need to identify which certificate file you require to distribute the new release from App Center.
Which file type should you upload to App Center?

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

Answer: C

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/

Q71. 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. an Azure Scheduler job
B. a trigger
C. a gate
D. an Azure function

Answer: C

Explanation:
Scenarios and use cases for gates include:
Quality validation. Query metrics from tests on the build artifacts such as pass rate or code coverage and deploy only if they are within Required thresholds. Use Quality Gates to integrate monitoring into your pre-deployment or post deployment. This ensures that you are meeting the key health/performance metrics (KPIs) as your applications move

from dev to production and any differences in the infrastructure environment or scale is not negatively impacting your KPIs. Note: Gates allow automatic collection of health signals from external services, and then promote the release when all the signals are successful at the same time or stop the deployment on timeout. Typically, gates are used in connection with incident management, problem management, change management, monitoring, and external approval systems.
References: https://docs.microsoft.com/en-us/azure/azure-monitor/continuous-monitoring
https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates?view=azuredevops

Q72. 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. the Microsoft Test & Feedback extension
B. Microsoft Visual Studio App Center integration
C. Azure Application Insights widgets
D. Jenkins integration

Answer: B

Q73. 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. Grunt
B. Chef
C. Maven
D. Gulp

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

Q74. 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 conditions
B. deployment queue settings
C. release gates
D. pull request triggers

Answer: B

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/enus/azure/devops/pipelines/process/stages?tabs=classic&view=azure-devops#Queuinghttps://docs.microsoft.com/enus/azure/devops/pipelines/process/stages?tabs=classic&view=azure-devops - Queuing-policiespolicies

Q75. 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. integration testing
B. staging
C. production release
D. build

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/

Q76. You have a GitHub repository.
You create a new repository in Azure DevOps.
You need to recommend a procedure to clone the repository from GitHub to Azure DevOps.
What should you recommend?

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

Answer: D

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

Q77. 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

Correct Answer: D
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/Implement DevOps Development Processes

Q78. 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*

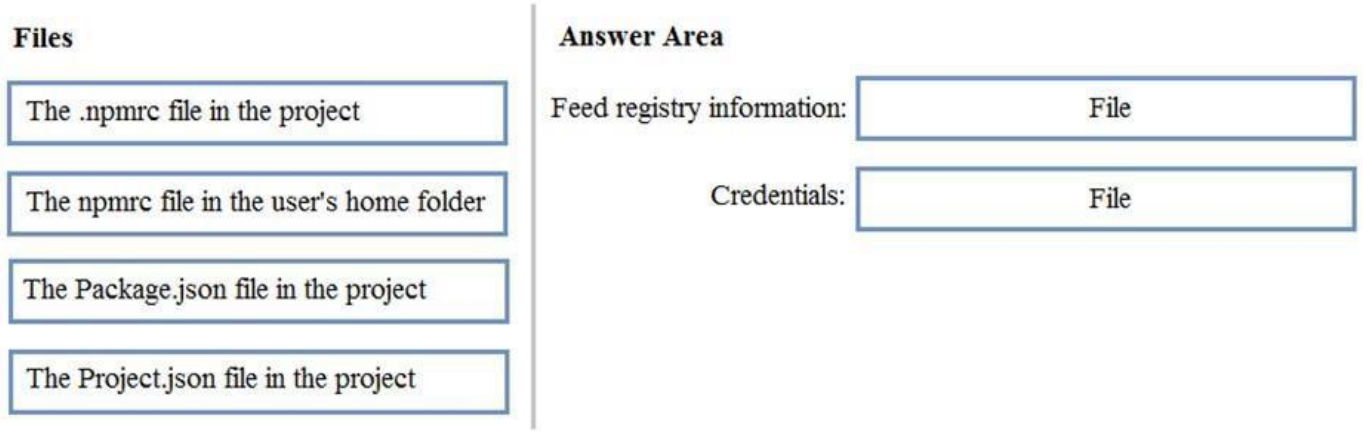
What should you include in the recommendation?

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

Answer: A

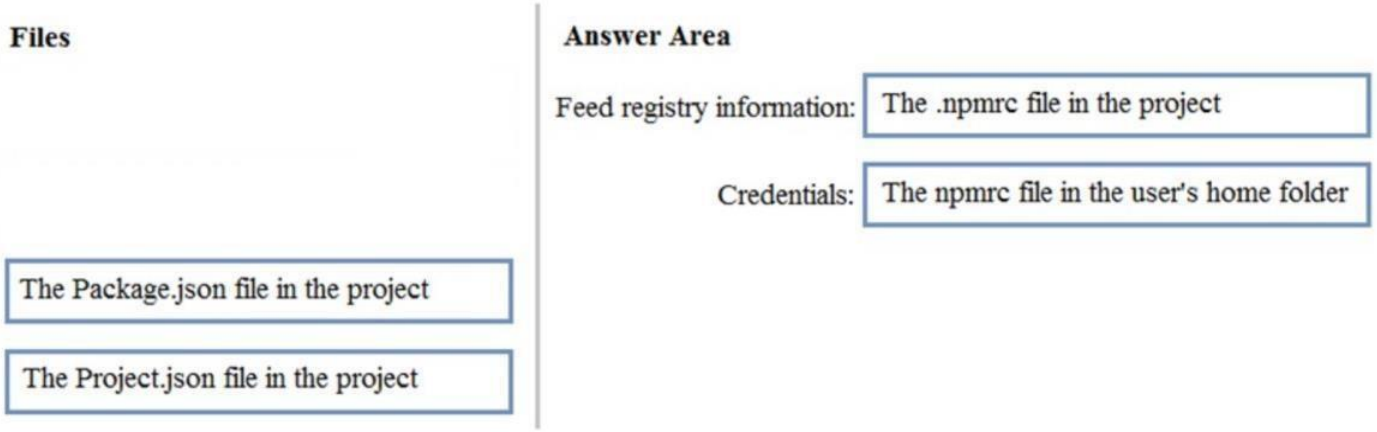
Explanation:
The Custom Script Extension downloads and executes scripts on Azure virtual machines. This extension is useful for post deployment configuration, software installation, or any other configuration or management tasks. Scripts can be downloaded from Azure storage or GitHub, or provided to 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

Q79. 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.



A. The .npmrc file in the project
B. The .npmrc file in the user's home folder
C. The Package.json file in the project
D. The Project.json file in the project

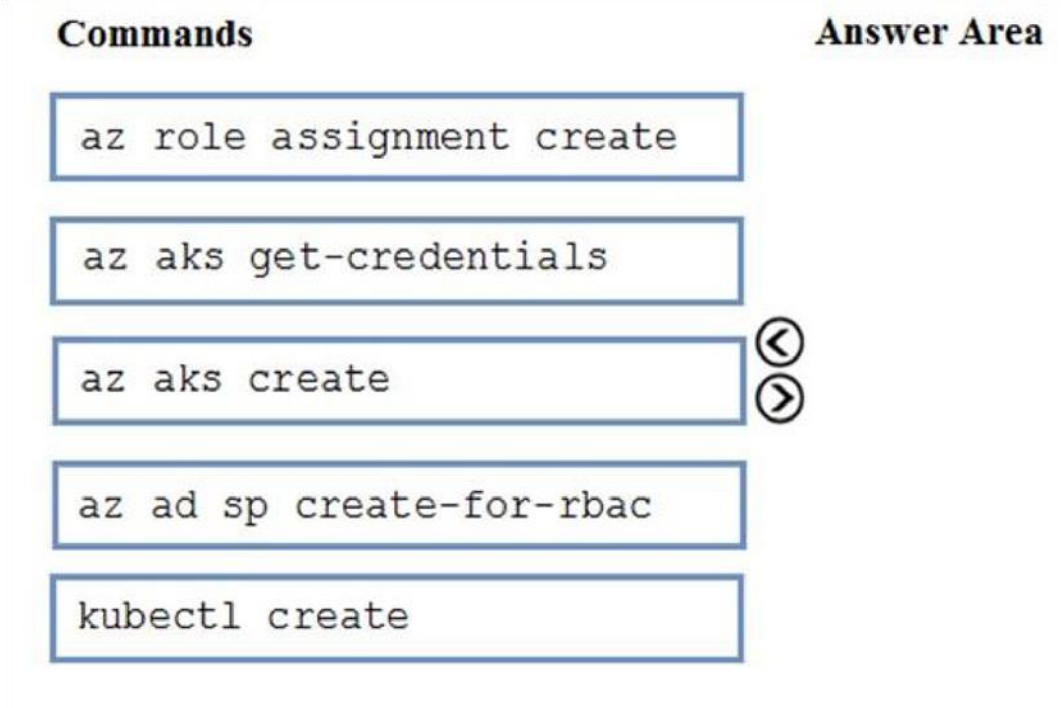
Answer: AB



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=azuredevops&tabs=windows

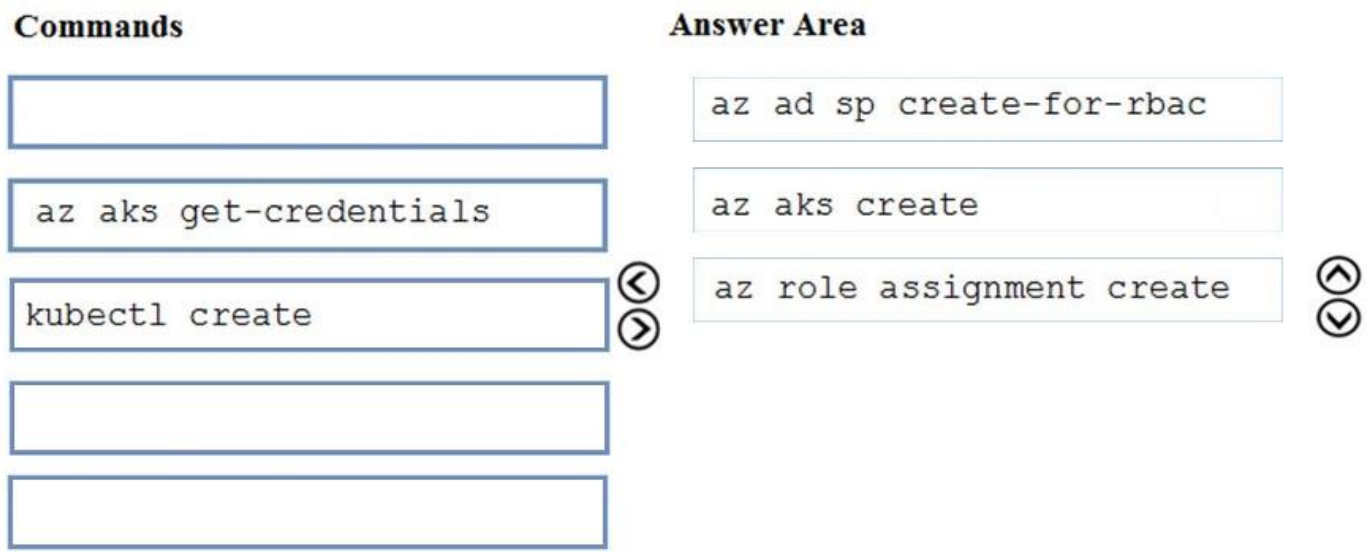
Q80. Drag and Drop question
You plan to use Azure Kubernetes Service (AKS) to host containers deployed from images hosted in a Docker Trusted Registry.

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.



A. az role assignment create[3]
B. az aks get-credentials
C. az aks create[2]
D. az ad sp create-for-rbac[1]
E. kubectl create

Answer: DCA



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

Q81. 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

Q82. Case Study 1 - Litware
Overview

Existing Environment
Litware, Inc. e 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.

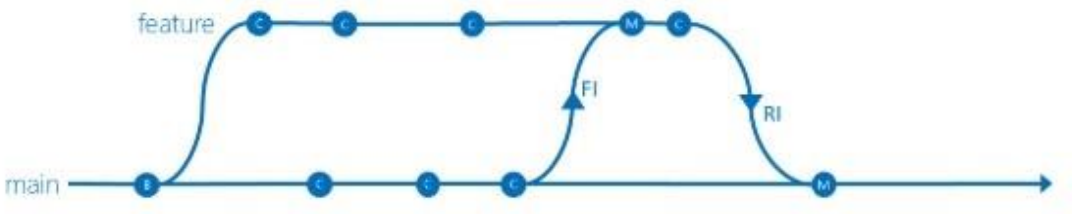
Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use.
By default, all releases must remain available for 30 days, except for production releases, which must be kept for 60 days.
Code Quality and release Quality are critical. During release, 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.
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-withtfvc?view=azure-devops

Q83. Case Study 1 - Litware
Overview
Existing Environment
Litware, Inc. e 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.

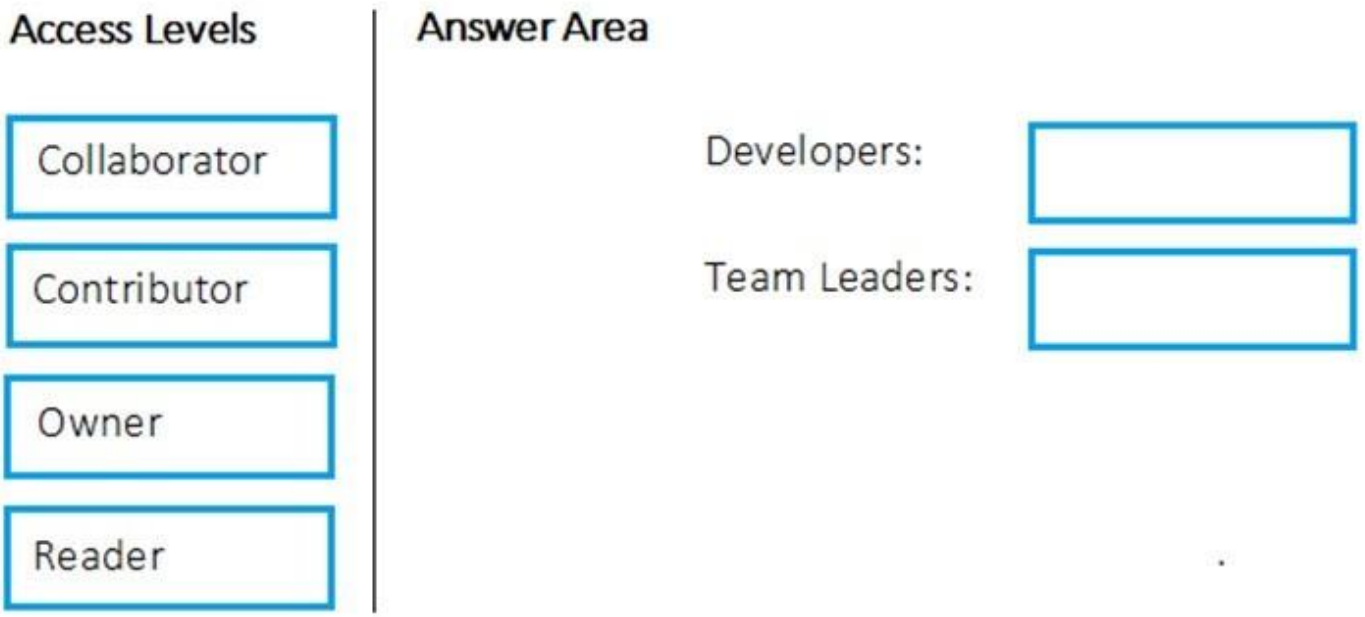
A branching strategy that supports developing new functionality in isolation must be used.
Members of a group named Team Leaders must be able to create new packages and edit the permissions of package feeds.
Visual Studio App Center must be used to centralize the reporting of mobile application crashes 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.

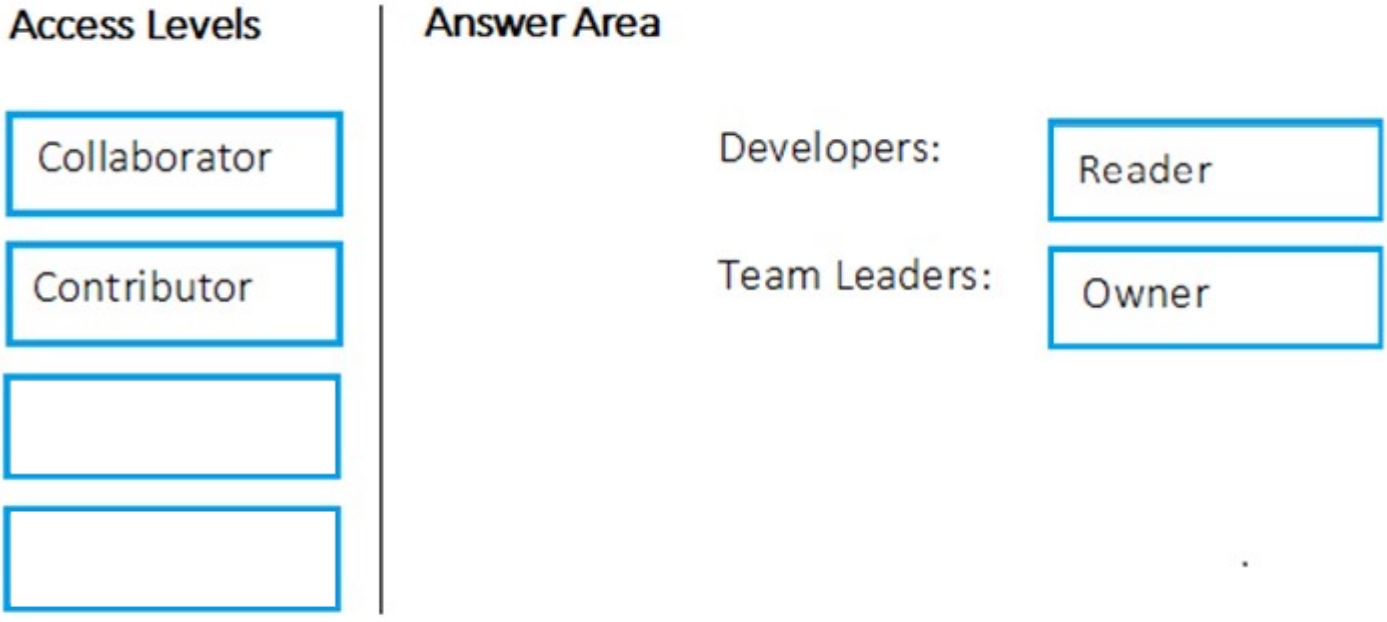
```
Register-AzureRmAutomationDscNode
  -ResourceGroupName 'TestResourceGroup'
  -AutomationAccountName 'LitwareAutomationAccount'
  -AzureVMName $vmanme
  -ConfigurationMode 'ApplyOnly'
```

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.



A. Collaborator
B. Contributor
C. Owner[2]
D. Reader[1]

Answer: DC



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.

Q84. 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

Q85. 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.

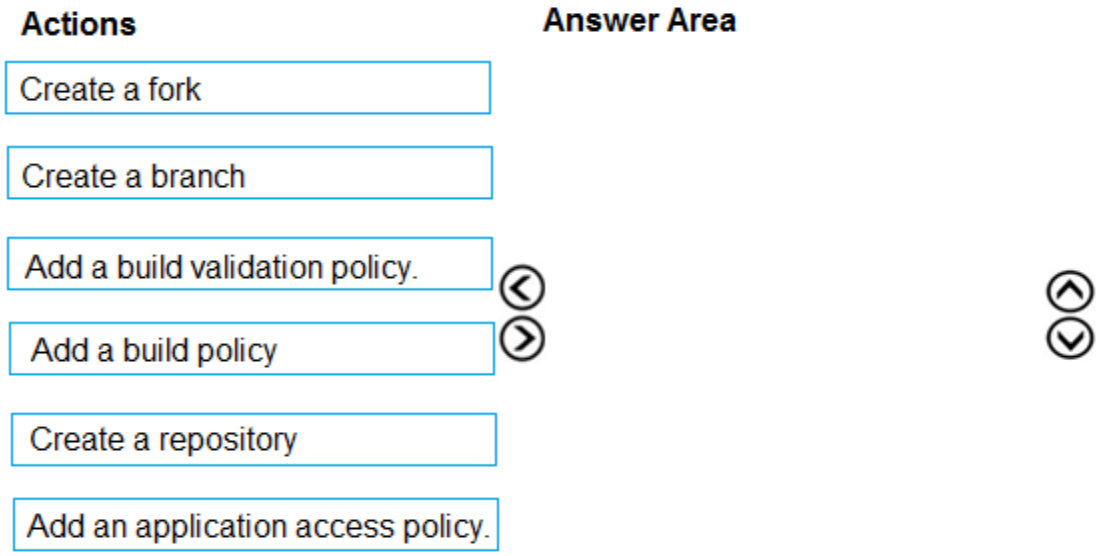
Technical Requirements
Contoso identifies the following technical Requirements:
Implement build agents for Project1.
Whenever possible, use Azure resources.

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.

QUESTION:

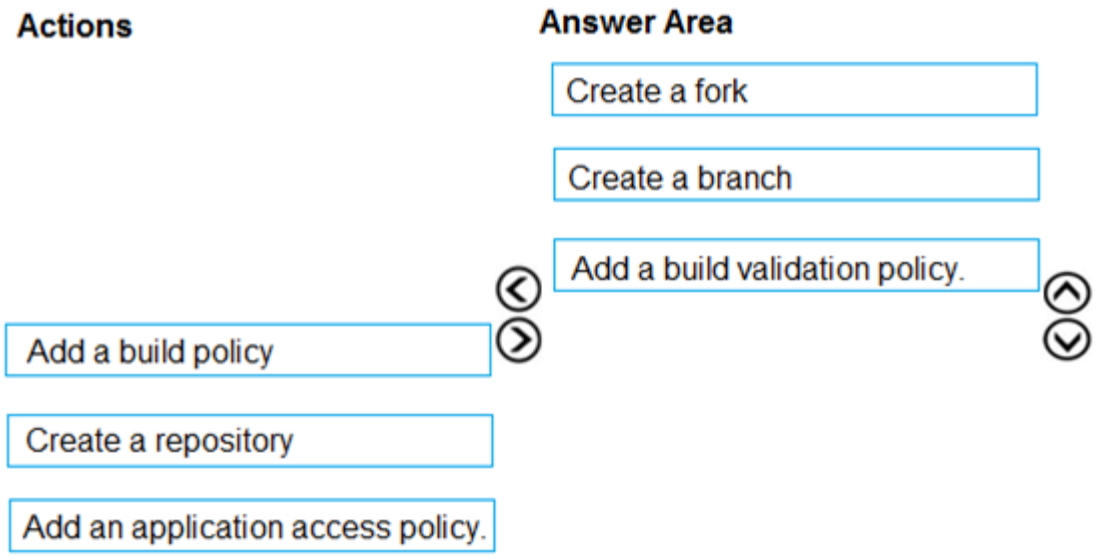
Drag and Drop
You need to implement the code flow strategy for Project2 in Azure DevOps.

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



A. Create a fork[1]
B. Create a branch[2]
C. Add a build validation policy[3]
D. Add a build policy
E. Create a repository
F. Add an application access policy

Answer: ABC



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

Q86. 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.

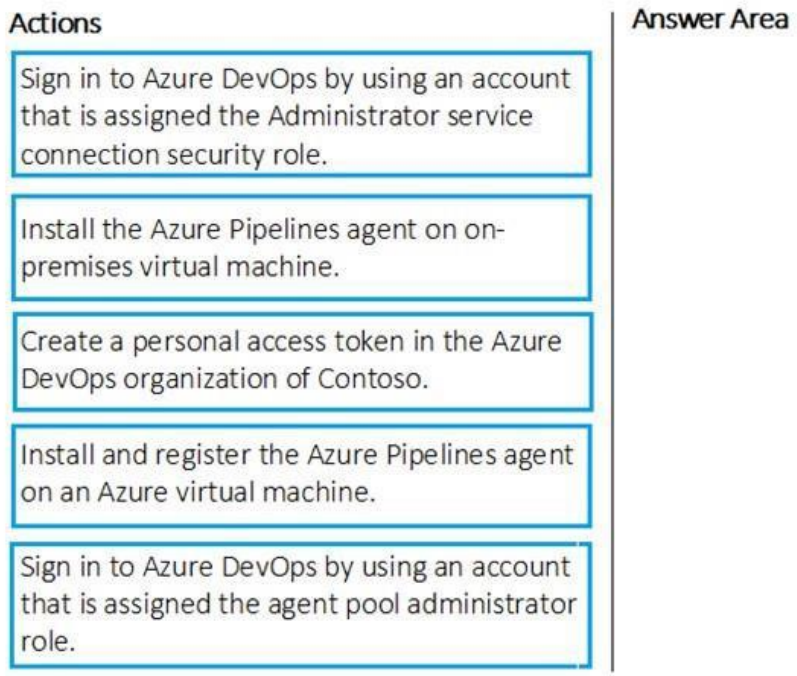
Project name	Project details
Project 1	Project1 will provide support for incremental builds and third-party SDK components
Project 2	Project2 will use an automatic build policy. A small team of developers named Team2 will work independently on changes to the project. The Team2 members will not have permissions 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.*

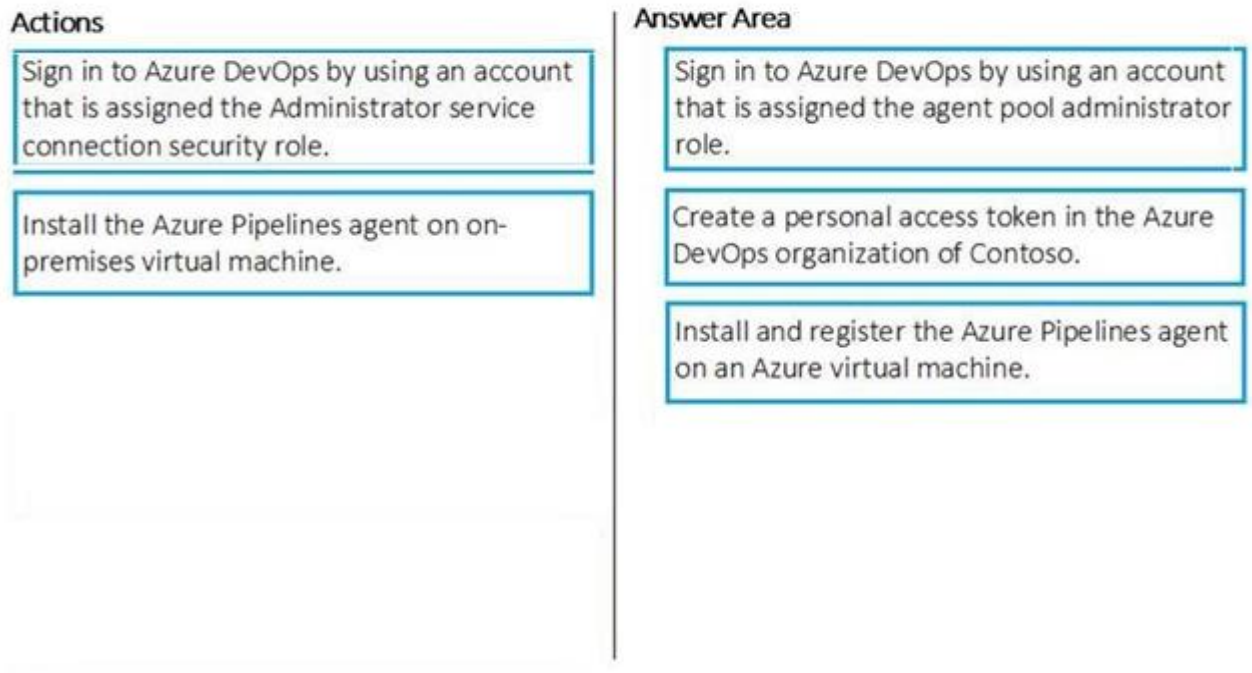
Whenever possible implement automation and minimize administrative effort.
Implement Project3, Project5, Project6, and Project7 based on the planned changes Implement Project4 and configure the project to push Docker images to Azure Container Registry.

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.



A. Sign in to Azure Devops by using an account that is assigned the Administrator service connection security role
B. Install the Azure Pipelines agent on on-premises virtual machine
C. Create a personal access token in the Azure DevOps organization of Contoso
D. Install and register the Azure Pipelines agent on an Azure Virtual machine
E. Sign in to Azure DevOps by using an account that is assigned the agent pool administrator role.

Answer: ECD



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-appwith-cicd-vsts https://mohitgoyal.co/2019/01/10/run-azure-devops-private-agents-in-kubernetes-clusters/

Q87. 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

Q88. 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

Q89. 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

Q90. 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

Q91. 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-testselenium?view=azure-devops

Q92. 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

Q93. 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

Q94. 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 Azure Key Vault task to the pipeline.

D. Add Azure Key Vault references to Azure Resource Manger templates.

Answer: D

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

Q95. 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

Q96. 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

Q97. 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: AB

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

Q98. 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

Q99. 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

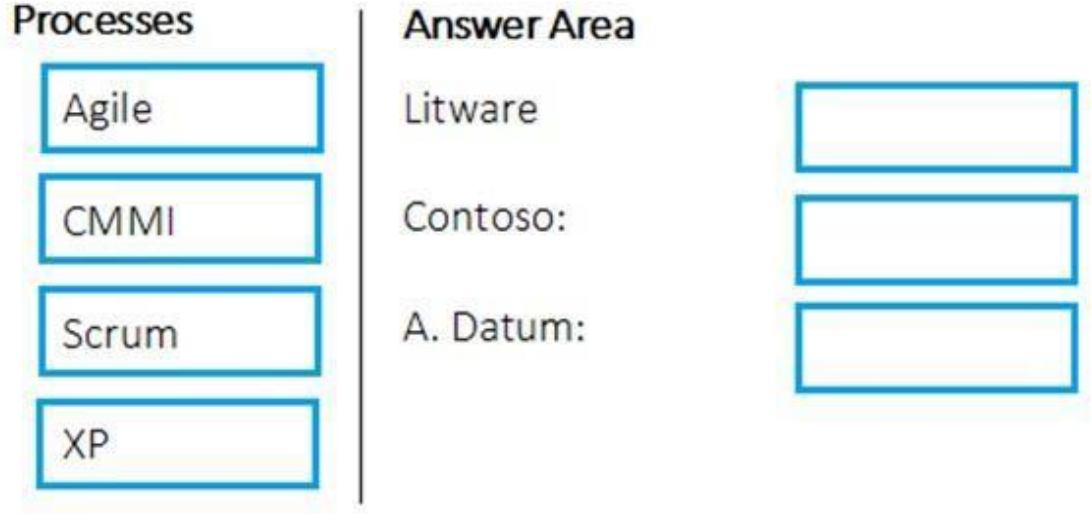
Explanation:
When releasing an iOS app signed with an ad-hoc or development provisioning profile, you must obtain tester's device IDs (UDIDs), and add them to the provisioning profile before compiling a release. When you enable the distribution group's Automatically manage devices setting, App Center 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

Q100. 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.

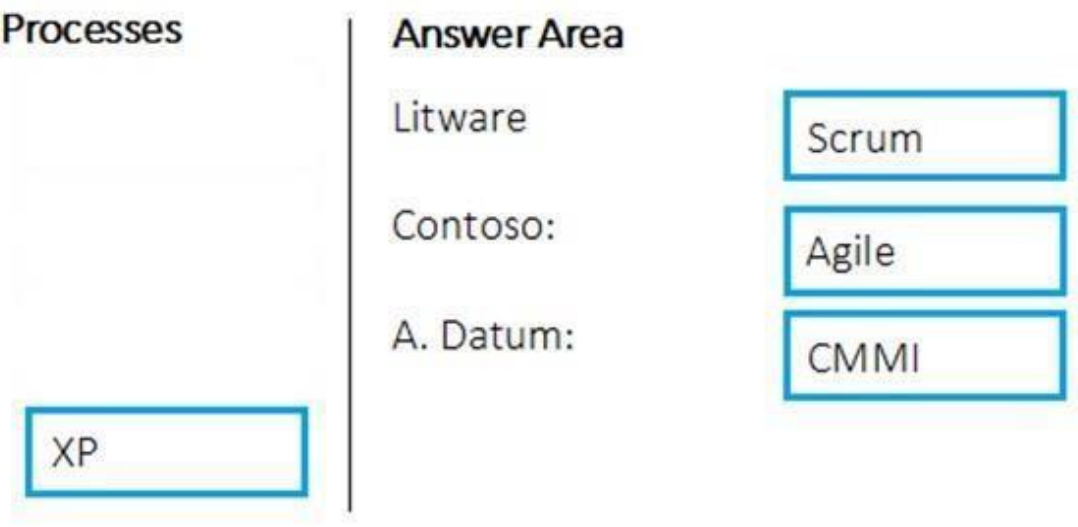
The customers all plan to use Azure DevOps for work item management.
Which work item process should you use for each customer? To answer, drag the appropriate work item process to the correct customers. Each work item process may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



A. Agile[2]
B. CMMI[3]
C. Scrum[1]
D. XP

Answer: CAB



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/chooseprocess?view=azure-devops

Q101. 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

Box1
A. " Microsoft.Resources/deployments"
B. " Microsoft.Resources/subscriptions"
C. " Microsoft.Resources/ subscriptions/resourceGroups"
Box2
D. "Append",
E. "Deny"'
F. "DeployIfNotExists",

Answer: CD

Answer Area

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-resourcegroups

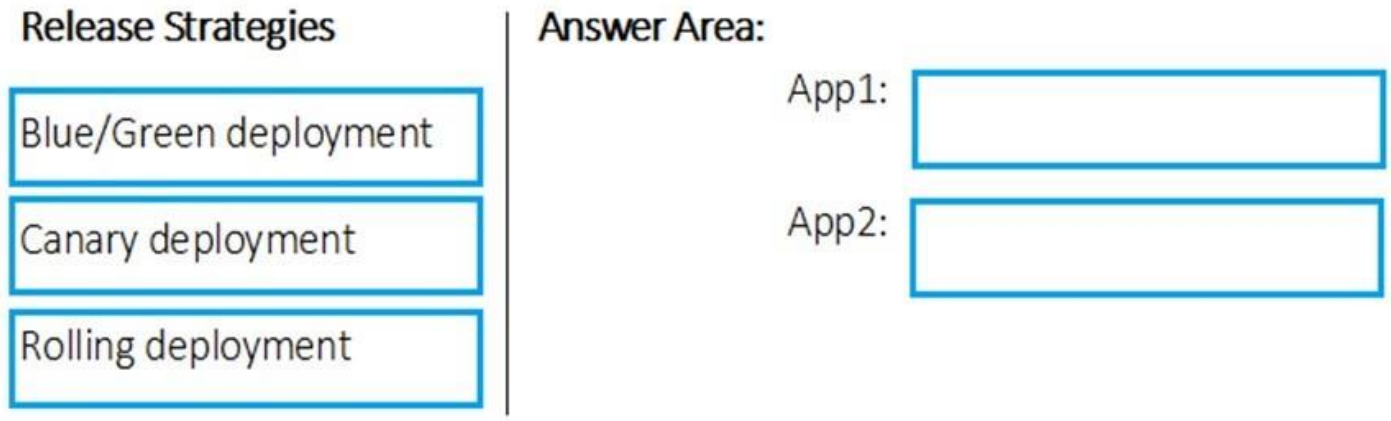
Q102. Drag and Drop question

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.

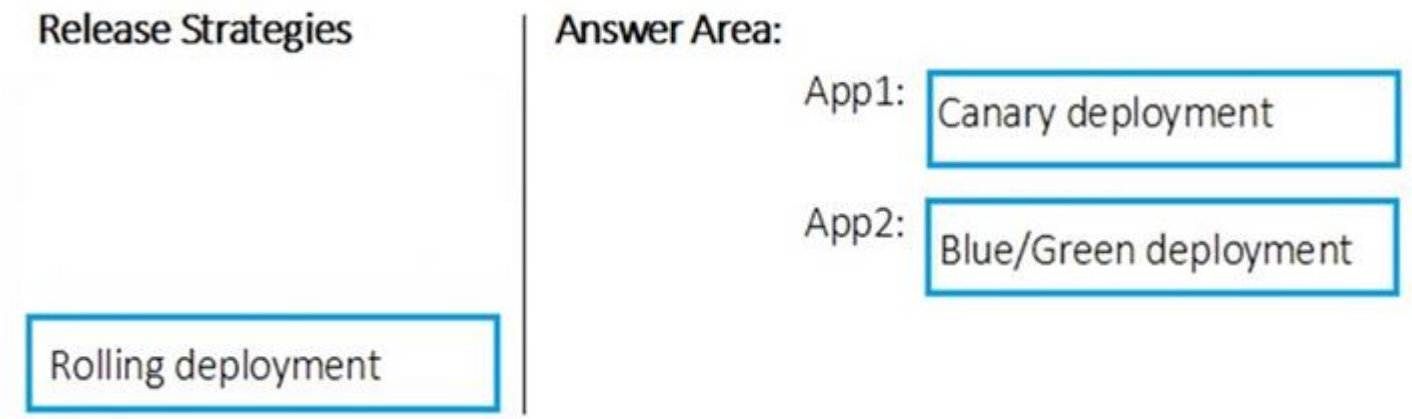
Which release strategy should you use for each application? To answer, drag the appropriate release strategies to the correct applications. Each release strategy may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



A. Blue/green deployment[2]
B. Canary deployment[1]
C. Rolling deployment:

Answer: BA

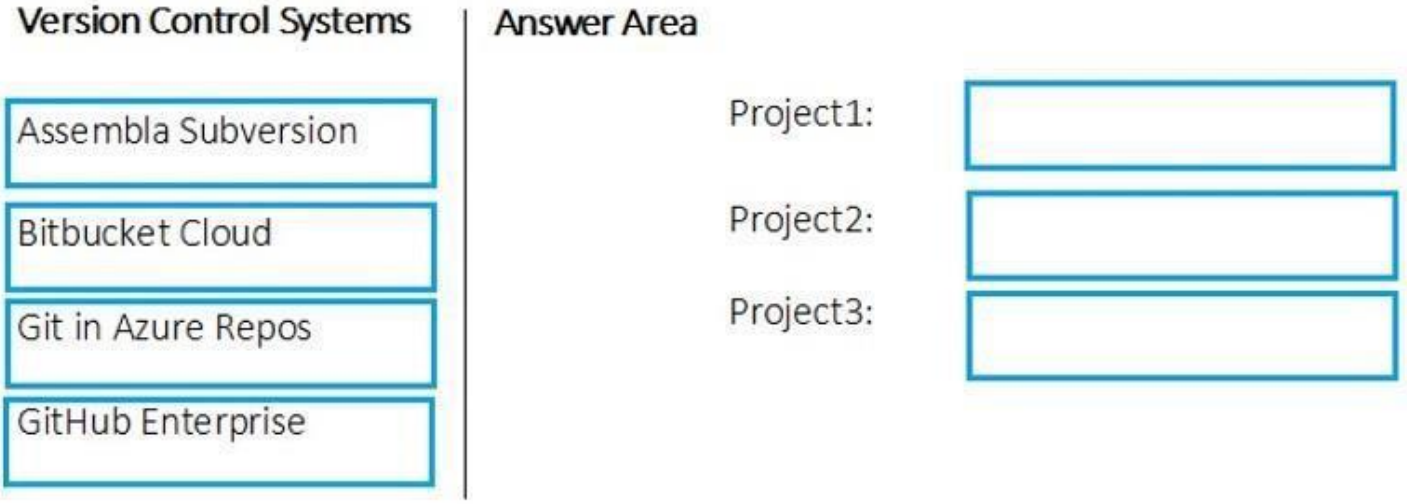


Explanation:
App1: Canary deployment
With canary deployment, you deploy a new application code in a small part of the production infrastructure. Once the application is signed off for release, only a few users are routed to it. This minimizes any impact.
With no errors reported, the new version can gradually 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

Q103. Drag and Drop question
You are configuring Azure Pipelines for three projects in Azure DevOps as shown in the following table.

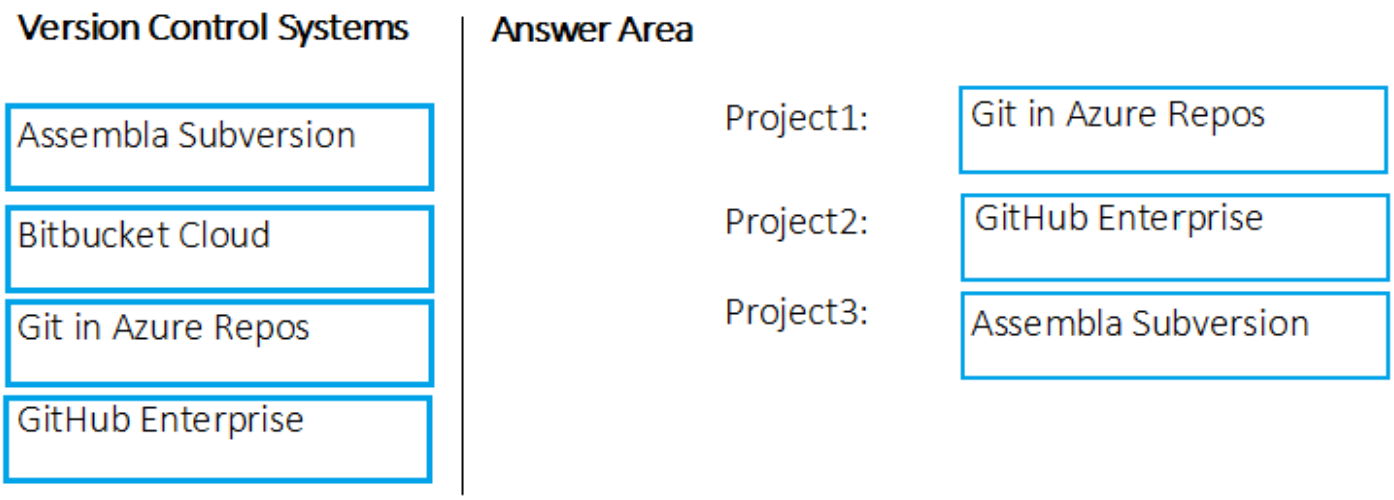
Project name	Project Details
Project1	The project team provides preconfigured YAML files that it wants to use to manage future pipeline configuration changes.
Project2	The sensitivity of the project requires that the source code be hosted on the managed Windows server on your company's network.
Project3	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.



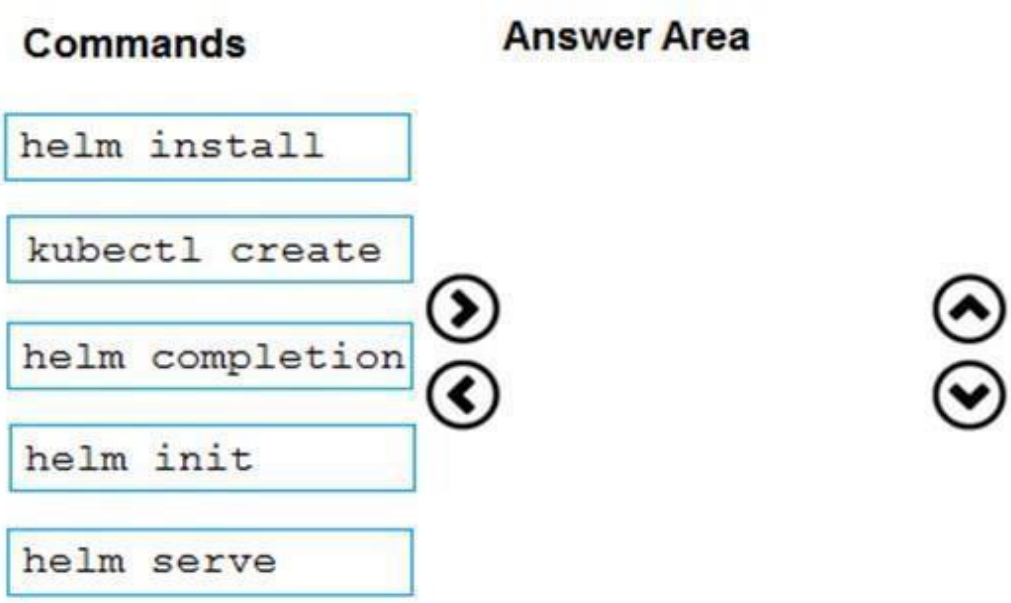
A. Assemble Subversion[3]
B. Bitbucket Cloud
C. Git in Azure Repos[1]
D. GitHub Enterprise[2]

Answer: CDA



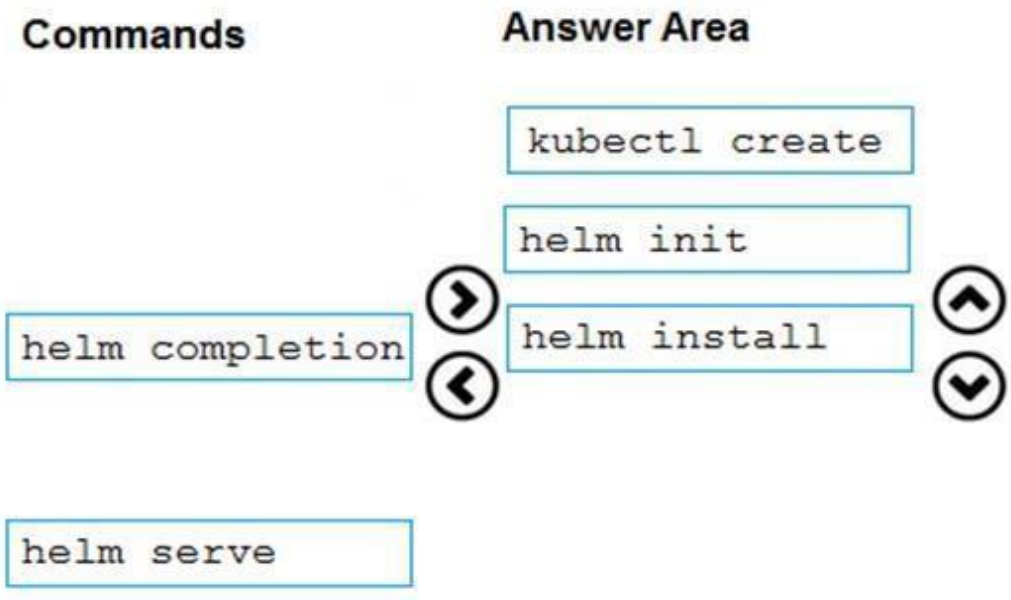
Explanation:
Project1:Git in Azure Repos
Project2: Github Enterprise
GitHub Enterprise is the on-premises version of GitHub.com. GitHub Enterprise includes the same great set of features as GitHub.com but packaged for running on your organization's local network. All repository data is stored on machines that you control, and access is integrated with your organization's authentication system (LDAP, SAML, or CAS).
Project3: Bitbucket cloud
One downside, however, is that Bitubucket does not include support for SVN but this can be easily amended migrating the SVN repos to Git with tools such as SVN Mirror for Bitbucket .
Note: SVN is a centralized version control system.
Incorrect Answers:
Bitbucket:
Bitbucket comes as a distributed version control system based on Git.
Note: A source control system, also called a version control system, allows developers to collaborate on code and track changes. Source control is an essential tool for multi-developer projects. Our systems support two types of source control: Git (distributed) and Team Foundation
Version Control (TFVC). TFVC is a centralized, client-server system. In both Git and TFVC, you can check in files and organize files in folders, branches, and repositories.
References: https://www.azuredevopslabs.com/labs/azuredevops/yaml/
https://enterprise.github.com/faQ

Q104. 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.



A. helm install[3]
B. kubectl create[1]
C. helm completion
D. helm init[2]
E. helm serve

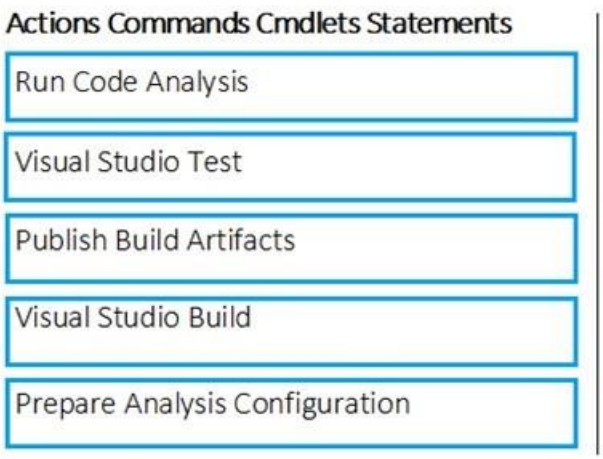
Answer: BDA



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.

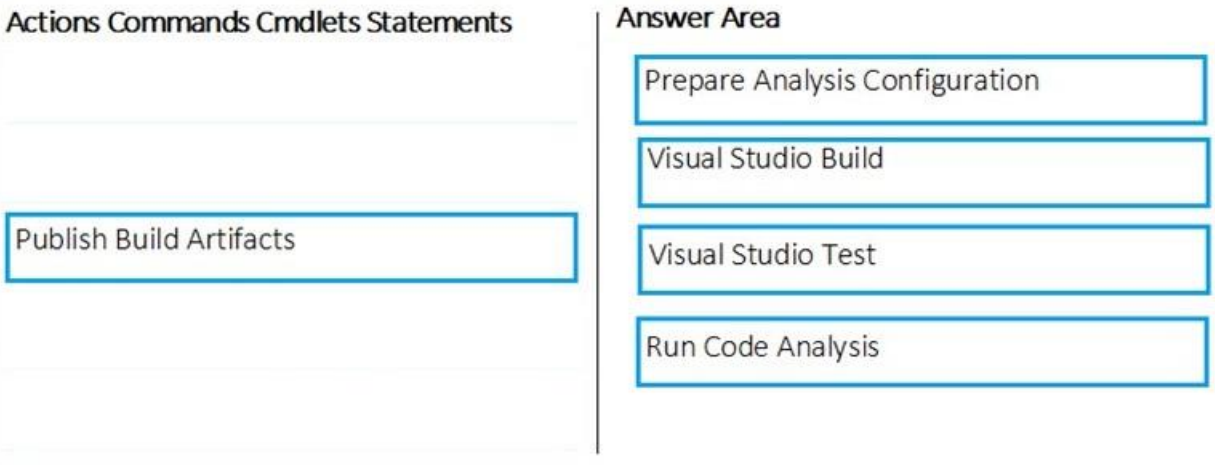
Example: Service account with cluster-admin role
$ kubectl create -f rbac-config.yaml serviceaccount "tiller" created clusterrolebinding "tiller" created $ helm init --service-account tiller
Step 2: helm init
To deploy a basic Tiller into an AKS cluster, use the helm init command.
Step 3: helm install
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

Q105. 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.



A. Run Code Analysis[4]
B. Visual Studio Test[3]
C. Publish Build Artifacts
D. Visual Studio Build[2]
E. Prepare Analysis Configuration[1]

Answer: EDBA



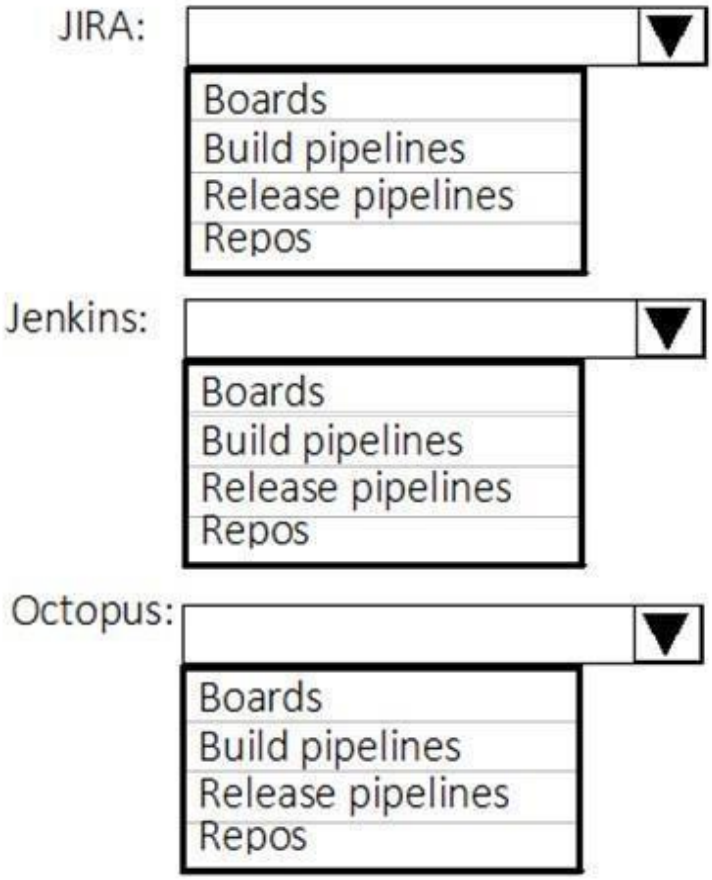
Explanation:

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

Q106. Hotspot question
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.

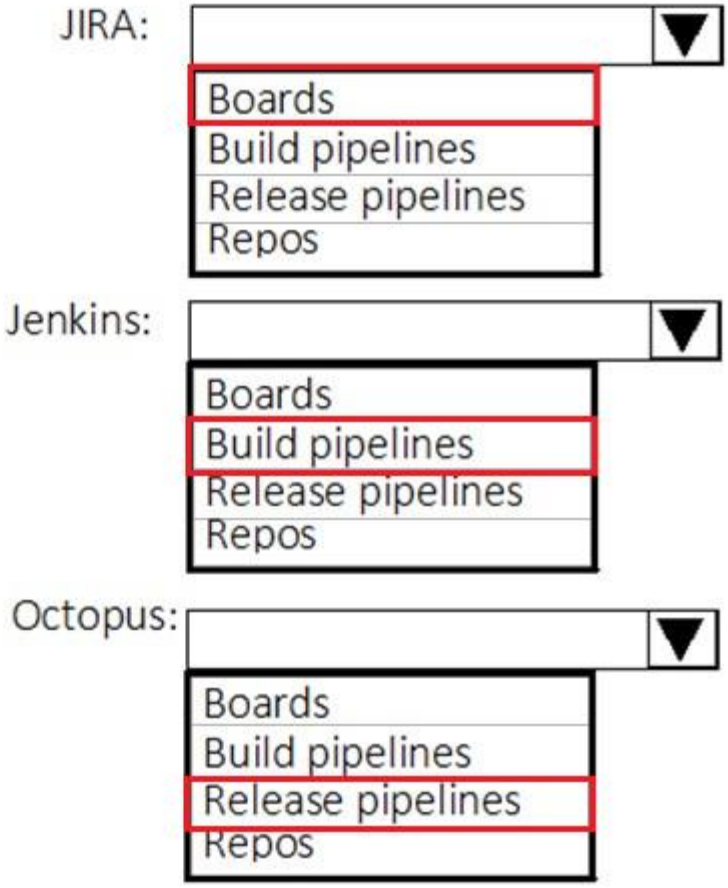
Answer Area



Box1
A. Boards
B. Build pipelines
C. Release pipelines
D. Repos
Box2
E. Boards
F. Build pipelines
G. Release pipelines
H. Repos
Box3
I. Boards
J. Build pipelines
K. Release pipelines
L. Repos

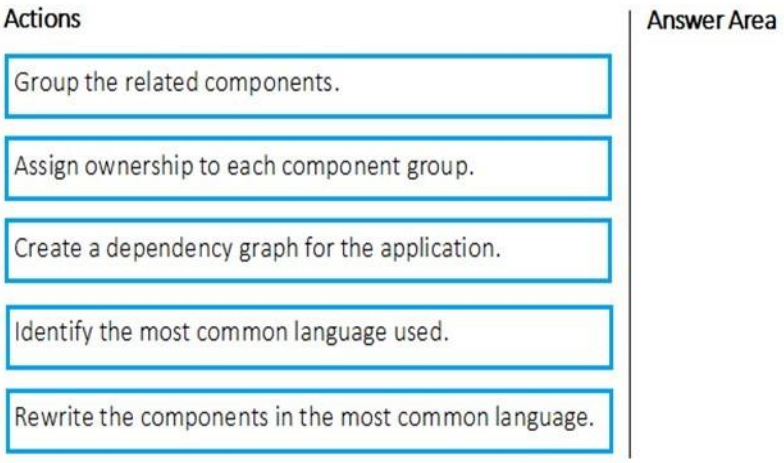
Answer: AFK

Answer Area



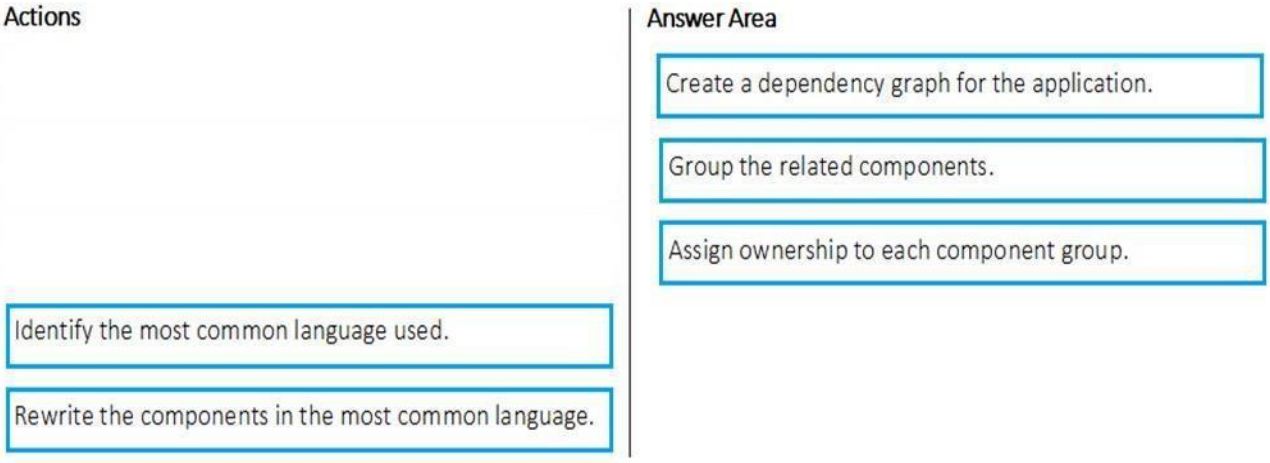
Explanation:
JIRA: Release pipelines
Atlassian's Jira Software is a popular application that helps teams to plan, track, and manage software releases, whereas Octopus Deploy helps teams automate their development and operations processes in a fast, repeatable, and reliable manner. Together, they enable 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/

Q107. 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.



A. Group the related components[2]
B. Assign ownership to each component group[3]
C. Create dependency graph for the application[1]
D. Identify the most common language used
E. Rewrite the components in the most common language

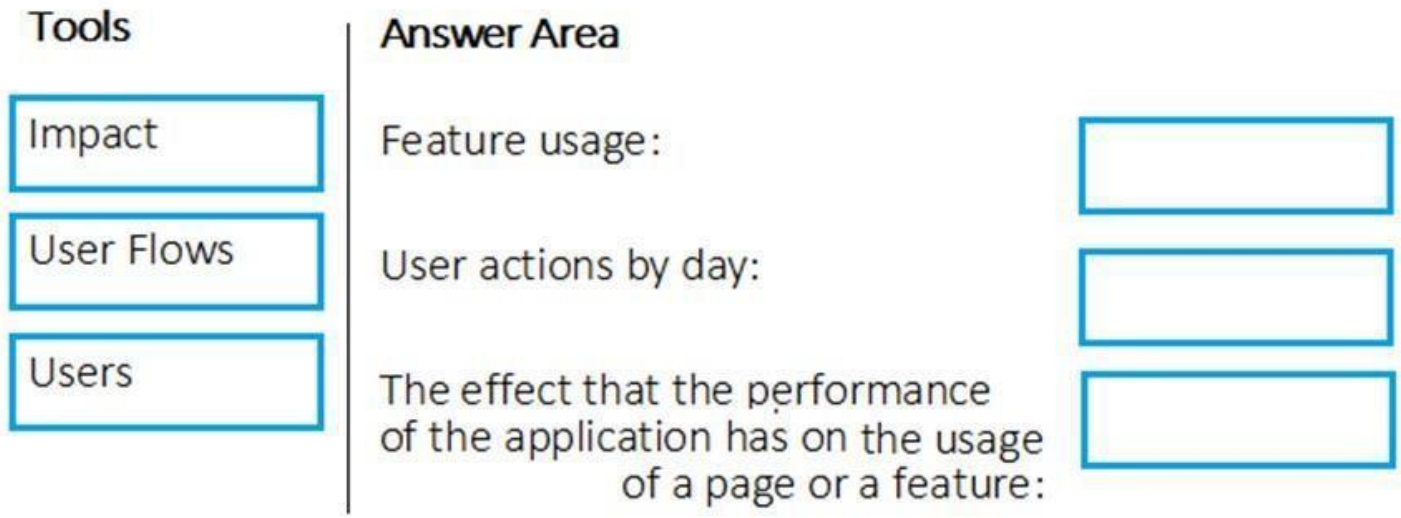
Answer: CAB



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-itemshttps://docs.microsoft.com/en-us/azure/devops/boards/Queries/link-work-items-supporttraceability?view=azure-devops&tabs=new-web-formsupporttraceability?view=azure-devops&tabs=new-web-form https://docs.microsoft.com/en-us/visualstudio/releasenotes/tfs2017-relnotes

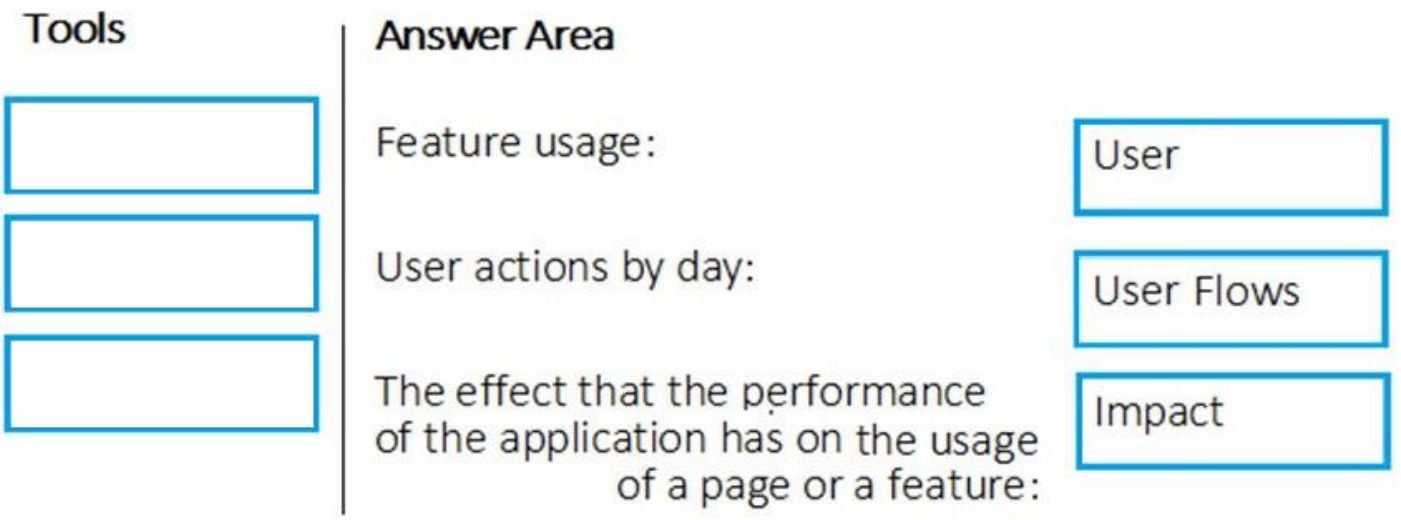
Q108. Drag and Drop question

Your company wants to use Azure Application Insights to understand how user behaviours affect an application.
Which application Insights tool should you use to analyze each behaviour? 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.



A. Impact[3]
B. User Flows[2]
C. Users[1]

Answer: BCA



Explanation:
Box 1: User
Box 2: The User Flows tool visualizes how users navigate between the pages and features of your site.
It's great for answering Qs 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 3: Impact
Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-flows

Q109.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: B

Q110. 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: A

Q111. 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

Q112. 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/

Q113. 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.ger.io/readiness-and-lieveness
       args:
       - /server
```

livenessProbe:
readinessProbe:
ShutdownProbe:
startupProbe:

```
    httpGet:
         path: /checknow
         port: 8123
         httpHeaders:
         - name: Custom-Header
           value: CheckNow
```

initialDelaySeconds: 15
periodSeconds: 15
timeoutSeconds: 15

Box1
A. livenessProbe:
B. readinessProbe:
C. shutdownProbe:
D. startupProbe:
Box2
E. initialDelay Seconds: 15
F. periodSeconds: 15
G.timeoutSeconds: 15

Answer: BF

Answer Area

```
apiVersion: v1
kind: Pod
metadata:
     labels:
          test: readiness-and-liveness
     name: readiness-http
spec:
     containers:
     - name: container1
       image: k8s.ger.io/readiness-and-lieveness
       args:
       - /server
```

[livenessProbe: | readinessProbe: | ShutdownProbe: | startupProbe:]

```
    httpGet:
         path: /checknow
         port: 8123
         httpHeaders:
         - name: Custom-Header
           value: CheckNow
```

[initialDelaySeconds: 15 | periodSeconds: 15 | timeoutSeconds: 15]

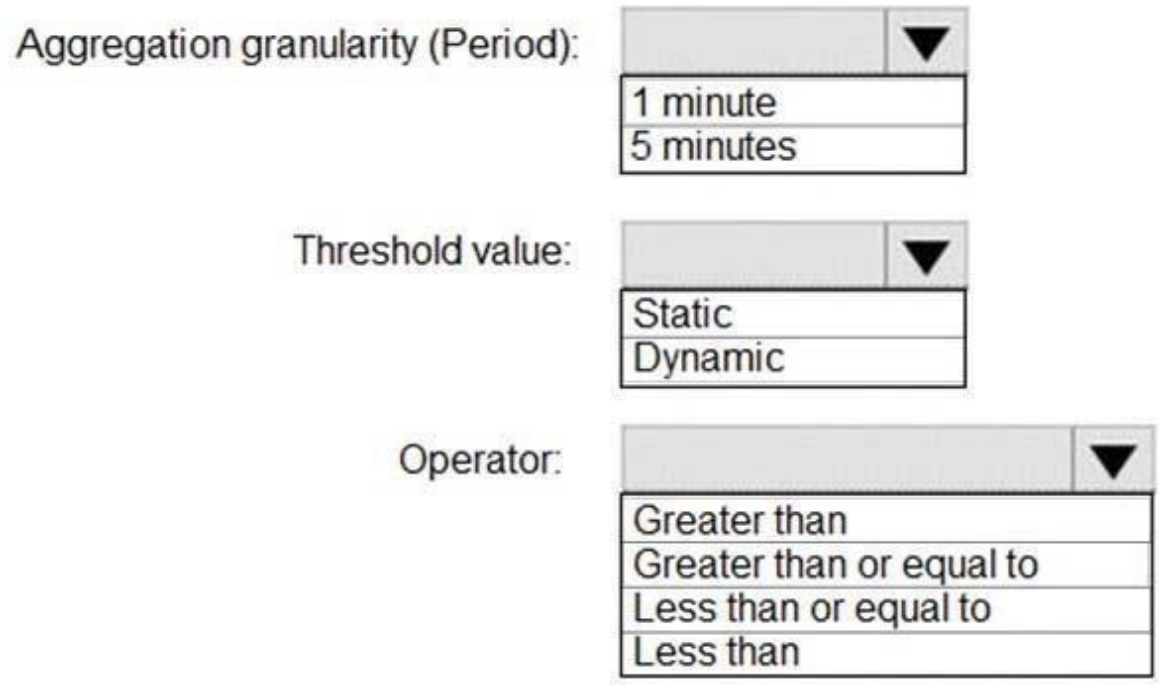
Explanation:
Box 1: readinessProbe:
For containerized applications that serve traffic, you might want to verify that your container is ready to handle incoming requests. Azure Container Instances supports readiness probes to include configurations so that your container can't be accessed under certain 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

Q114. 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.

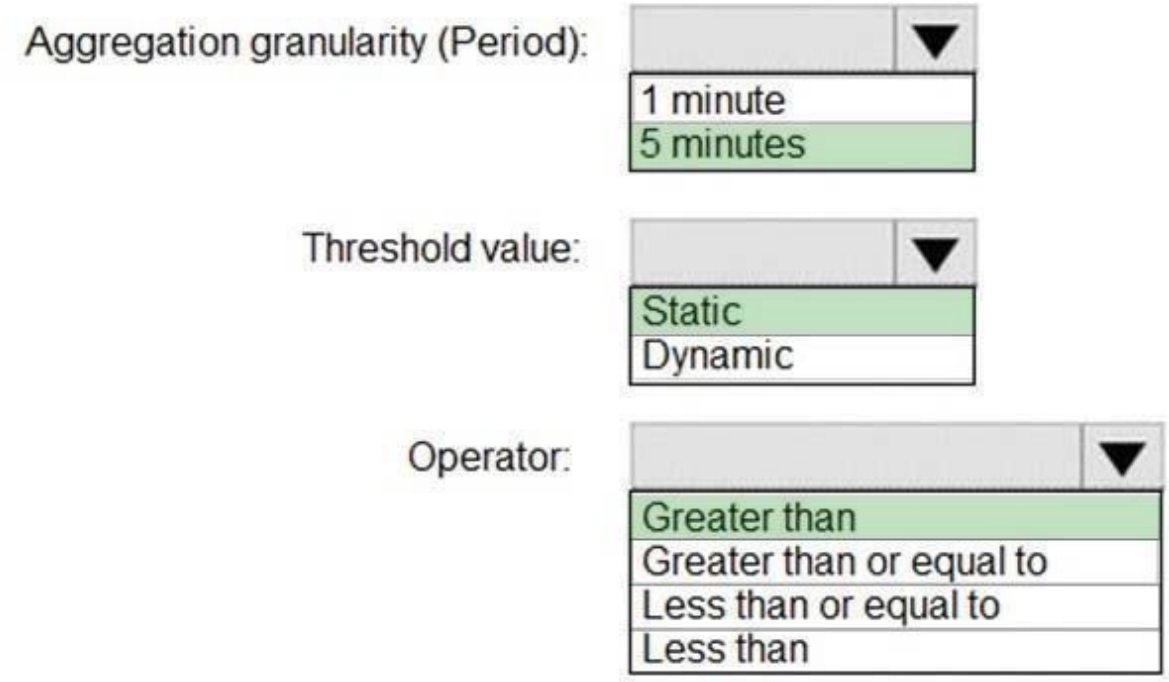
Answer Area



Box1
A. 1 minute
B. 5 minutes
Box2
C. Static
D. Dynamic
Box3
E. Greater than
F. Greater than or equal to
G. Less than or equal to
H. Less than

Answer: BCE

Answer Area



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

Q115. 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 selfhosted agent on on-premises computer(s).
Note 2: As we [Microsoft] are launching this new experience in preview, we are currentlyoptimizing 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

Q116. 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 selfhosted agent on on-premises computer(s).
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops

Q117. You have an Azure DevOps project.
Your build process creates several artifacts.
You need to deploy the artifacts to on-premises servers.
Solution: You deploy an Azure self-hosted agent to an on-premises server. You add a Copy and Publish Build Artifacts task to the deployment pipeline.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
To build your code or deploy your software using Azure Pipelines, you need at least one agent.
If your on-premises environments do not have connectivity to a Microsoft-hosted agent pool (which is typically the case due to intermediate firewalls), you'll need to manually configure a selfhosted agent on on-premises computer(s). The agents must have connectivity to the target onpremises 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

Q118. 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

Box1
A. feedback
B. signin
C. subscribe
D. subscription
Box2
E. https://dev.azure.com/contoso/contoso-app
F. https://dev.azure.com/contoso/contoso-app/core-api
G. https://dev.azure.com/contoso/contoso-app/core-db
H. https://dev.azure.com/contoso/contoso-app/core-spa

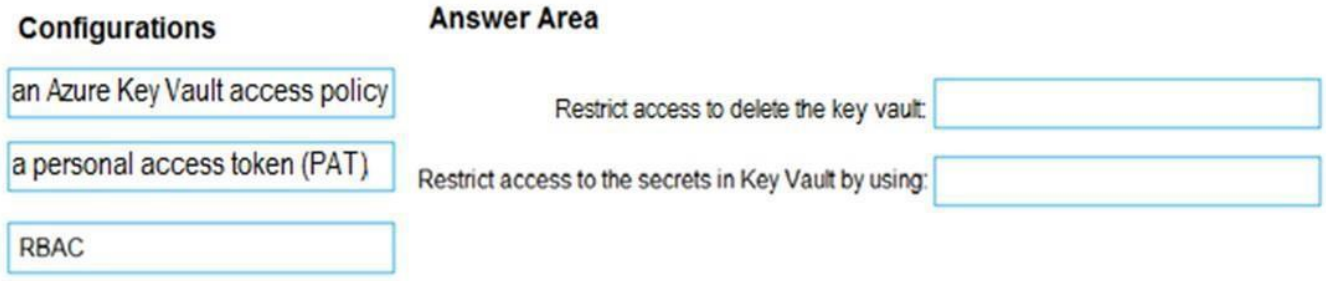
Answer: CE

Answer Area

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

Q119. 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.

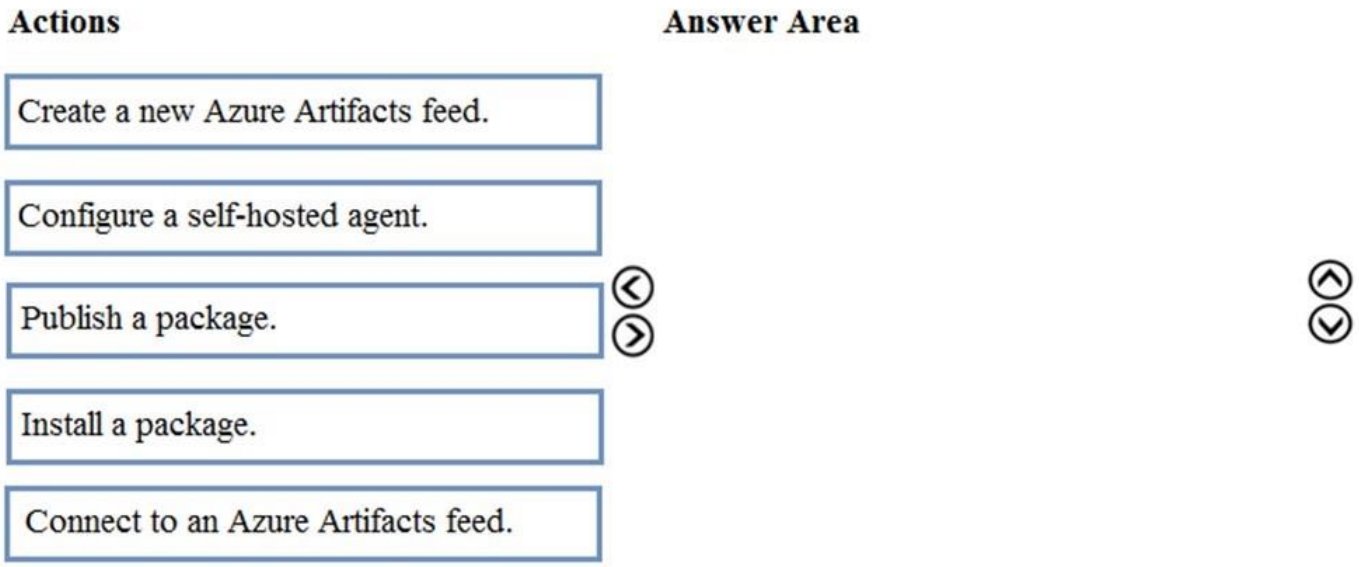


A. an Azure Key Vault access policy[2]
B. a personal access token (PAT)
C. RBAC[1]

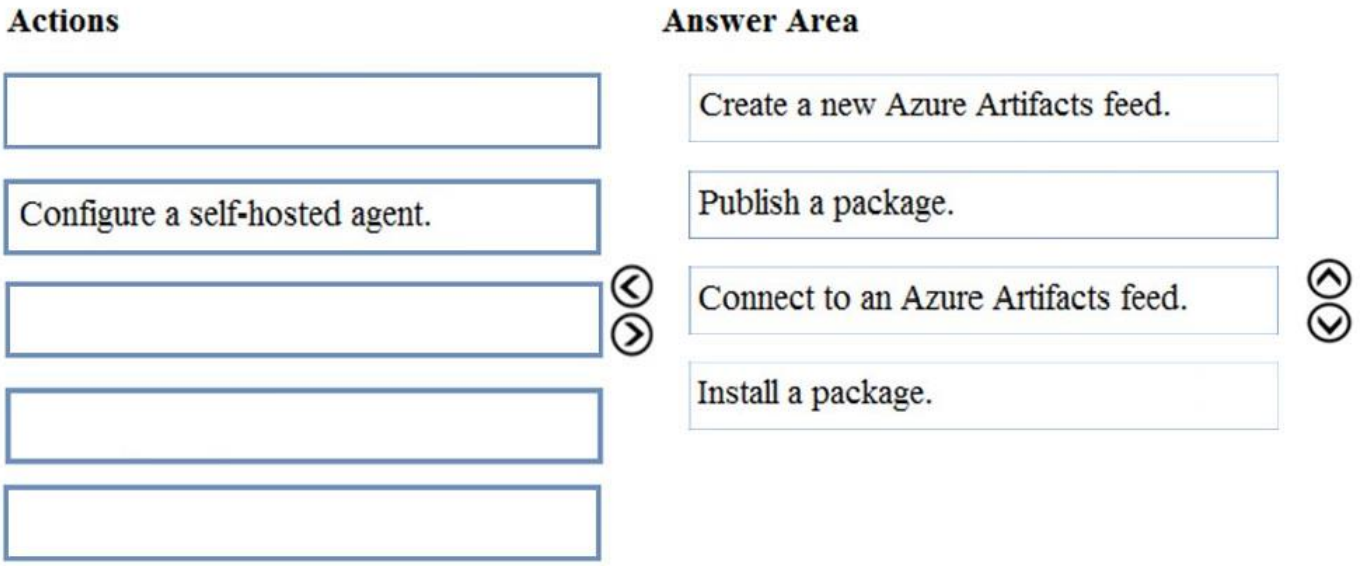
Answer: CA

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: Azure Key Vault access policy

Q120. 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.



A. Create a new Azure Artifacts feed[1]
B. Configure a self-hosted agent
C. Publish a package[2]
D. Install a package[4]
E. Connect to an Azure Artifacts feed[3]
Answer: ACDE

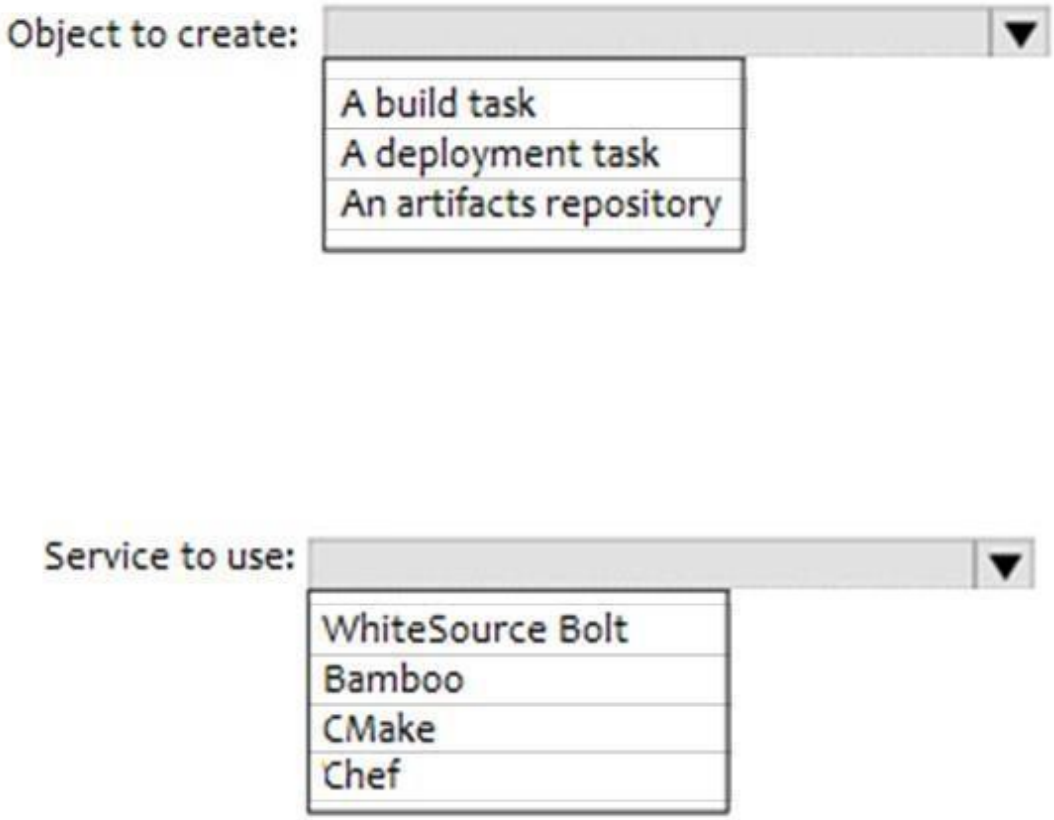


Explanation:
Step 1: Configure a self-hosted agent.
The build will run on a Microsoft hosted agent.

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-azurehttps://medium.com/@dan.cokely/creating-nuget-packages-in-azure-devops-with-azure-pipelinesand- yaml-d6fa30f0f15pipelinesand- yaml-d6fa30f0f15e

Q121. 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.

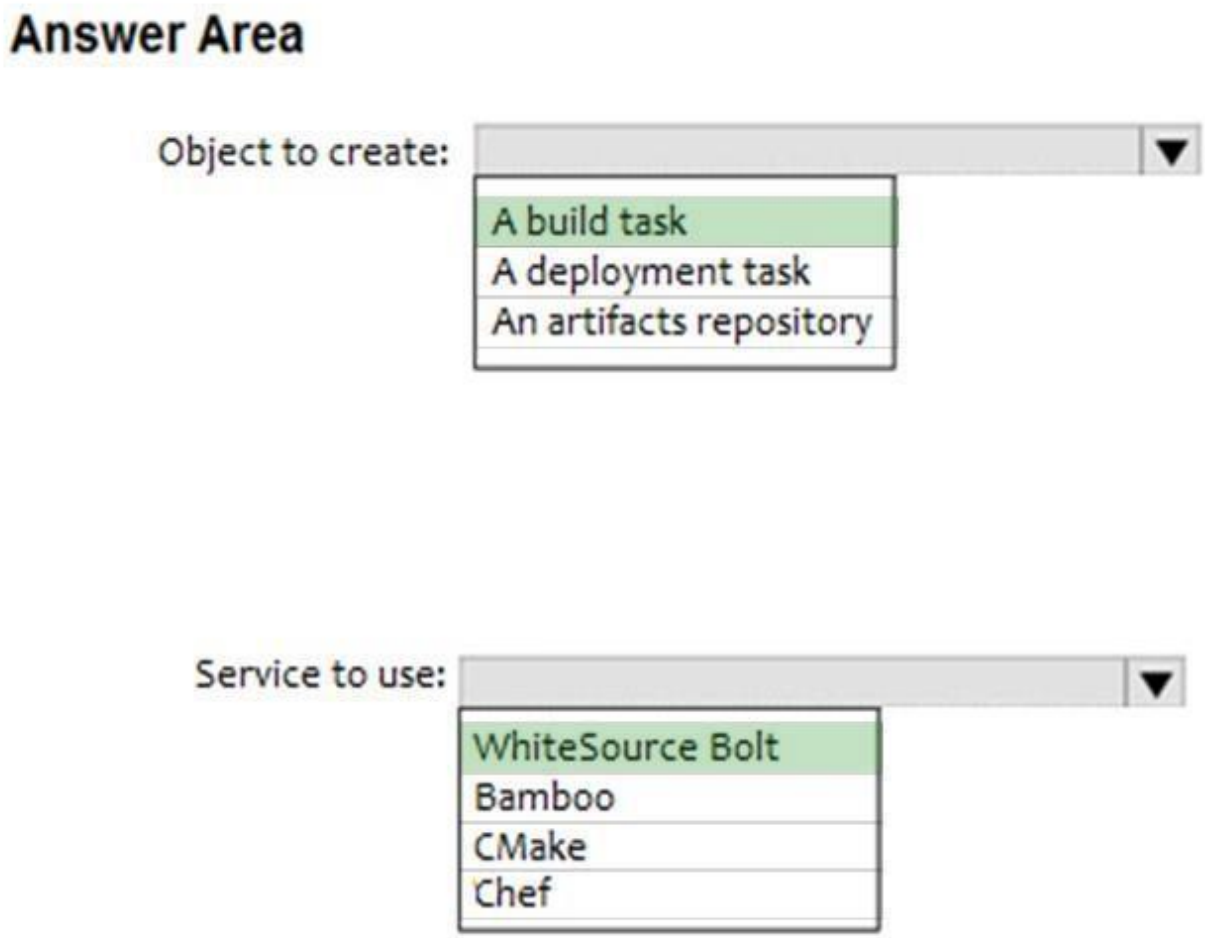
Answer Area



Box1
A. A build task
B. A deployment task
C. An artifacts repository
Box2
D. WhiteSource Bolt

E. Bamboo
F. CMake
G. Chef

Answer: AD



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/

Q122. Case Study 1 - Litware
Overview
Existing Environment
Litware, Inc. e an independent software vendor (ISV). Litware has a main office and five branchoffices. 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.

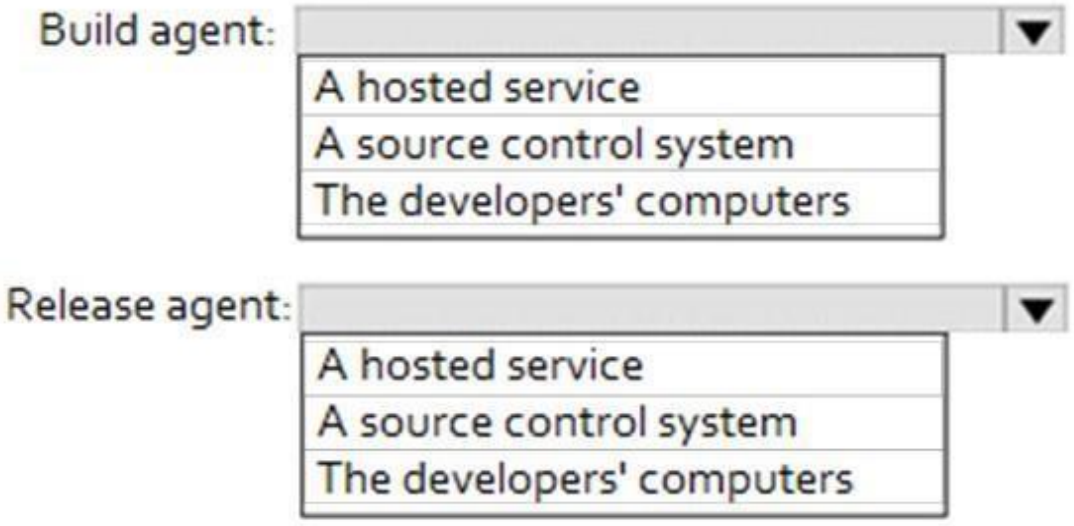
Current Technical Issue
The test servers are configured correctly when first deployed, but they experience configuration drift over time. Azure Automation State Configuration fails to correct the configurations.
Azure Automation State Configuration nodes are registered by using the following command.

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

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.

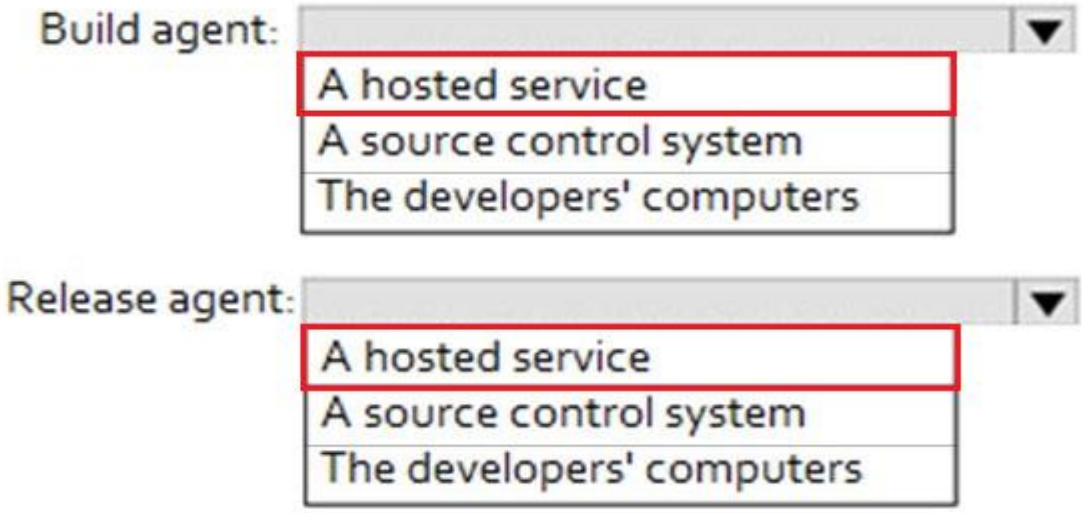
Answer Area



Box1
A. A hosted service
B. A source control system
C. The developer's computers
Box2
D. A hosted service
E. A source control system
F. The developer's computers

Answer: AD

Answer Area



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 selfhosted 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

Q123. 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

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/

Q124. 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

Q125. 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-dacpacdeployment

Q126. 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

Q127. 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

Q128. 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 predefined/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

Q129. 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

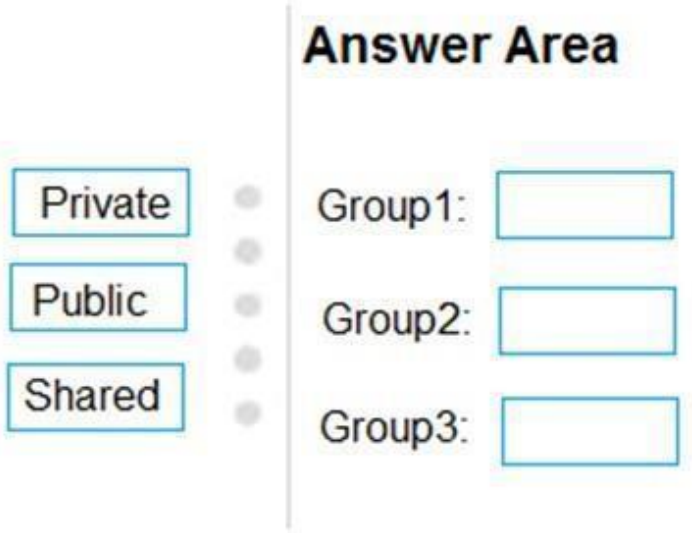
Explanation:
Before you can deploy Helm in an RBAC-enabled AKS cluster, you need a service account and role binding for the Tiller service.
Incorrect Answers:
C: Kubectl is a command line interface for running commands against Kubernetes clusters.
Reference:
https://docs.microsoft.com/en-us/azure/aks/kubernetes-helm

Q130. 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.



A. Private
B. Public
C. Shared

Answer: ABC

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

Q131. 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
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.
References: https://azure.microsoft.com/en-us/resources/container-security-in-microsoft-azure/en-us/

Q132. 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

Q133. 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/optimizewindows-dockerfile

Q134. 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.
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

Q135. 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.
References: https://azure.microsoft.com/en-us/services/devops/migrate/

Q136. 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

Q137. 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.
https://docs.microsoft.com/en-us/azure/aks/jenkins-continuous-deployment

Q138. A company currently uses ServiceNow for Incident and Change Management. Most of their webbased 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

Q139. 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

Q140. 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=azuredevops&tabs=windows

Q141. 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.
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/process/variables

Q142. 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.
References: https://www.atlassian.com/software/bamboo

Q143. 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?
(Choose 2)

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.
References: https://docs.microsoft.com/en-us/azure/devops/java/standalone-tools?view=azure-devops

Q144. 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

Q145. A team needs to create a Kubernetes cluster using the Azure CLI. The Kubernetes cluster needs to have monitoring enabled.
Which of the following would go into Slot2?

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

Answer: B

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

Q146. 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

Q147. 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.

Q148. 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

Q149. 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

Q150. 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

Q151. 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

Q152. 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

Q153. 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: EF

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

Q154. 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

Q155. 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

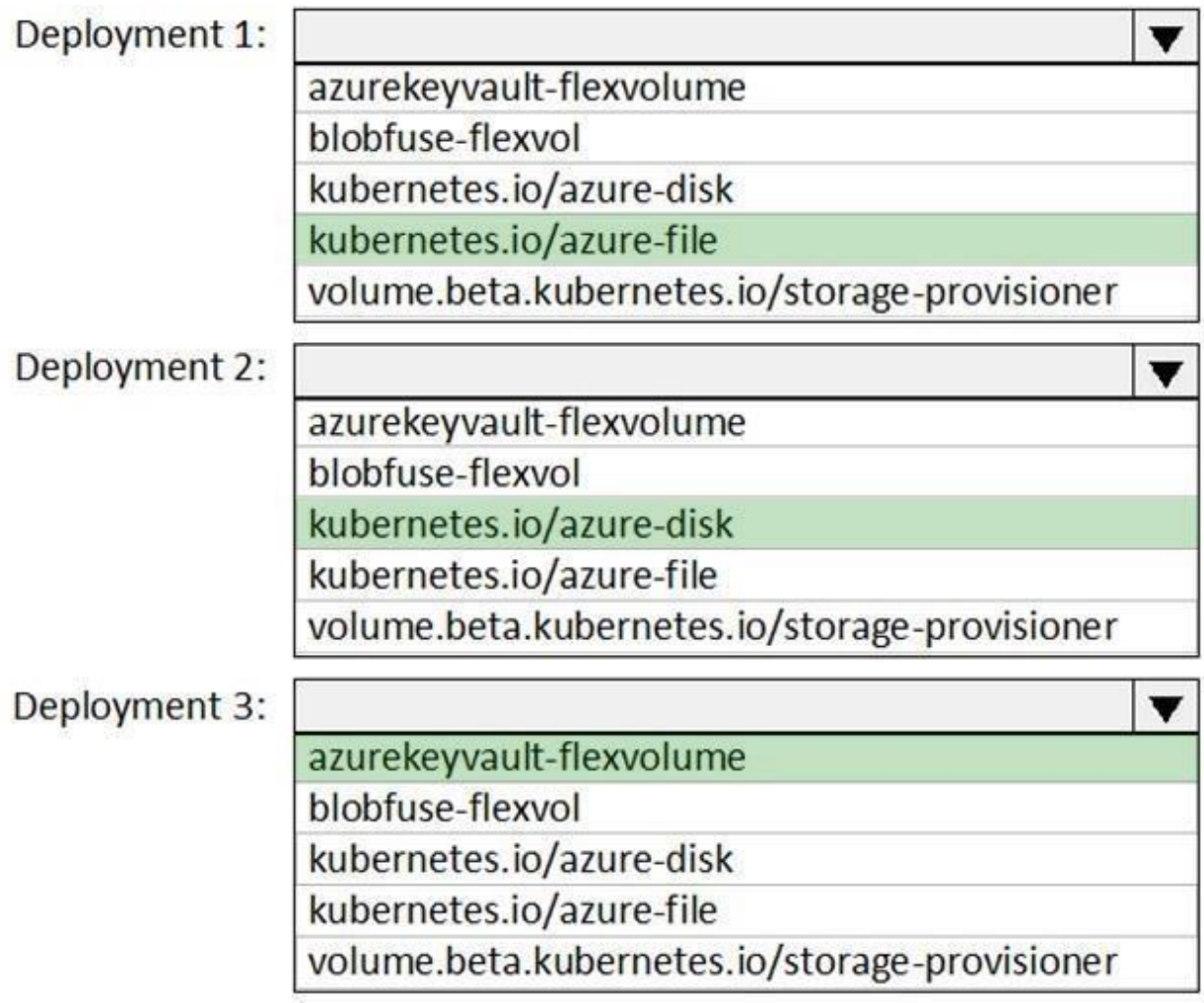
Deployment 3:
- azurekeyvault-flexvolume
- blobfuse-flexvol
- kubernetes.io/azure-disk
- kubernetes.io/azure-file
- volume.beta.kubernetes.io/storage-provisioner

Box1
A. azurekeyvault-flexvolume

B. blobfuse-flexvol
C. kubernetes.io/azure-disk
D. kubernetes.io/azure-file
E. volume.beta.kubernetes.io/storage-provisioner
Box2
F. azurekeyvault-flexvolume
G. blobfuse-flexvol
H. kubernetes.io/azure-disk
I. kubernetes.io/azure-file
J. volume.beta.kubernetes.io/storage-provisioner
Box3
K. azurekeyvault-flexvolume
L. blobfuse-flexvol
M. kubernetes.io/azure-disk
N. kubernetes.io/azure-file
O. volume.beta.kubernetes.io/storage-provisioner

Answer: DHK

Answer Area



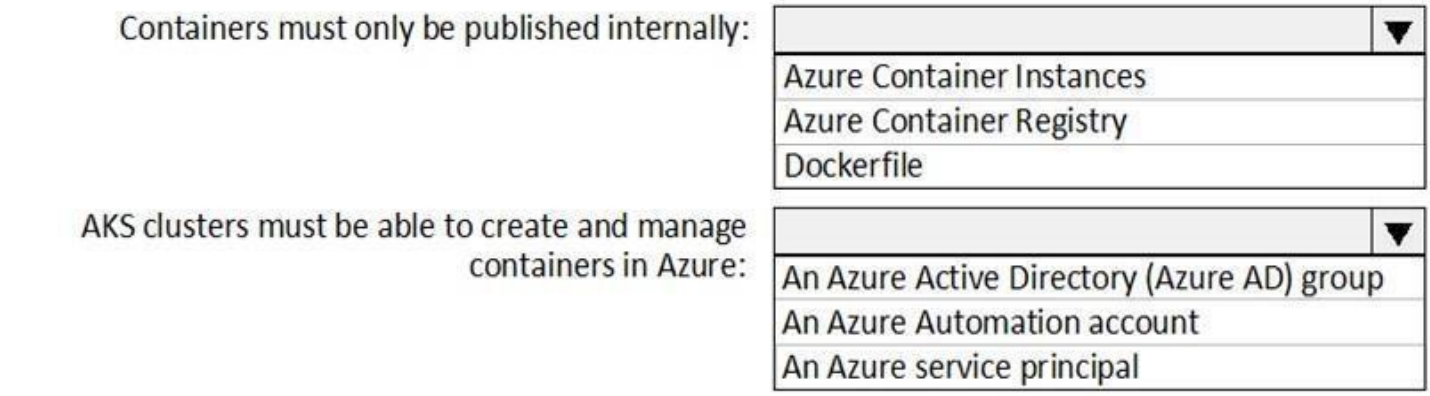
Explanation:
Deployment 1: Kubernetes.io/azure-file
You can use Azure Files to connect using the Server Message Block (SMB) protocol.
Deployment 2: Kubernetes.io/azure-disk Deployment 3: azurekeyvault-flexvolume azurekeyvault-flexvolume: Key Vault FlexVolume: Seamlessly integrate your key management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

Q156. 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.

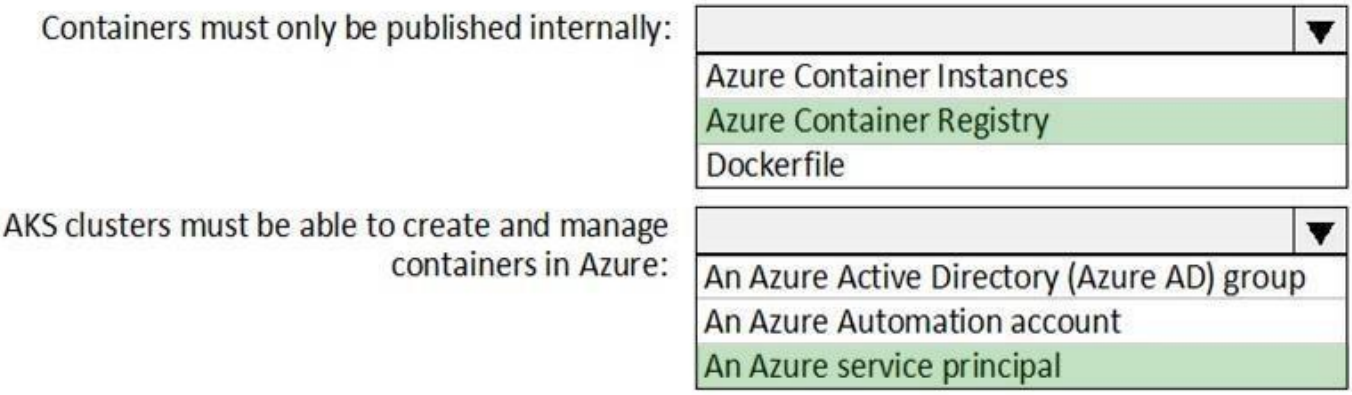
Answer Area



Box1
A. Azure Container Instances
B. Azure Container Registry
C. Dockerfile
Box2
D. An Azure Active Directory (Azure AD) group
E. An Azure Automation account
F. An Azure Service Principal

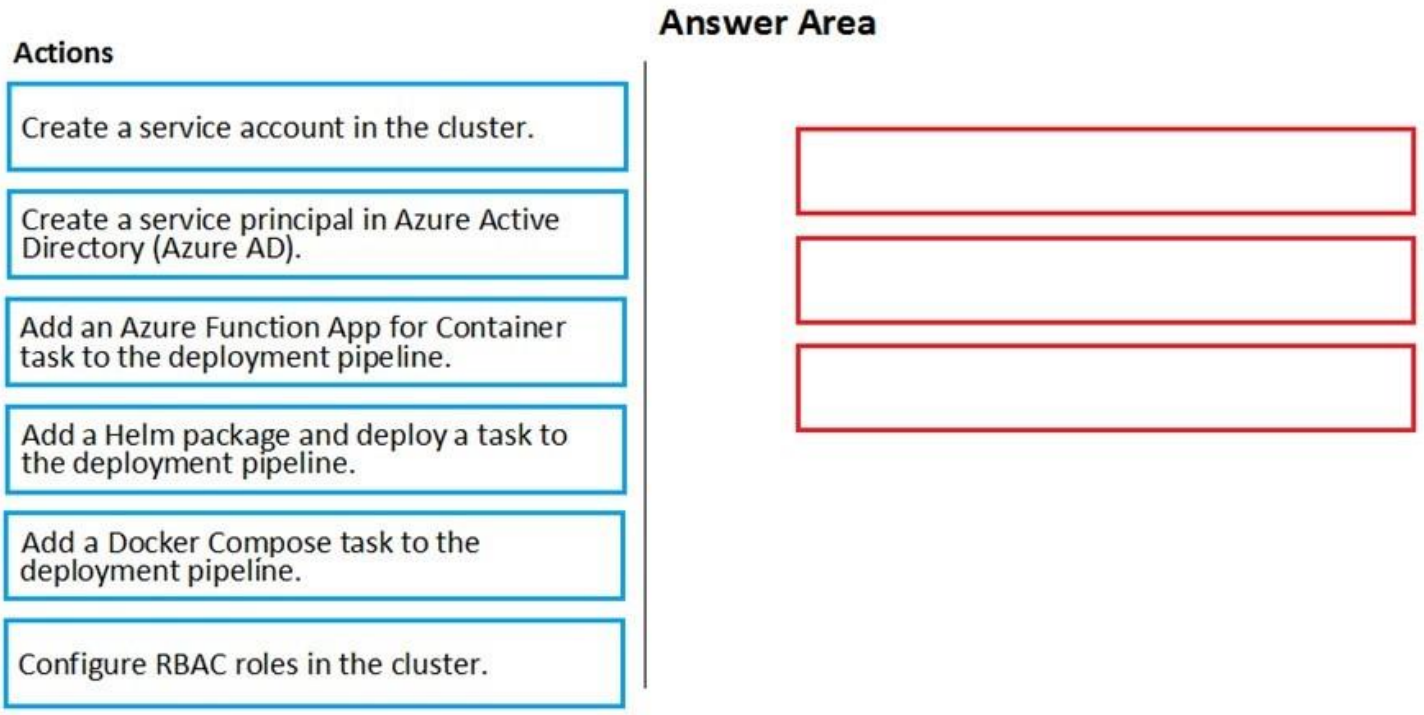
Answer: BF

Answer Area



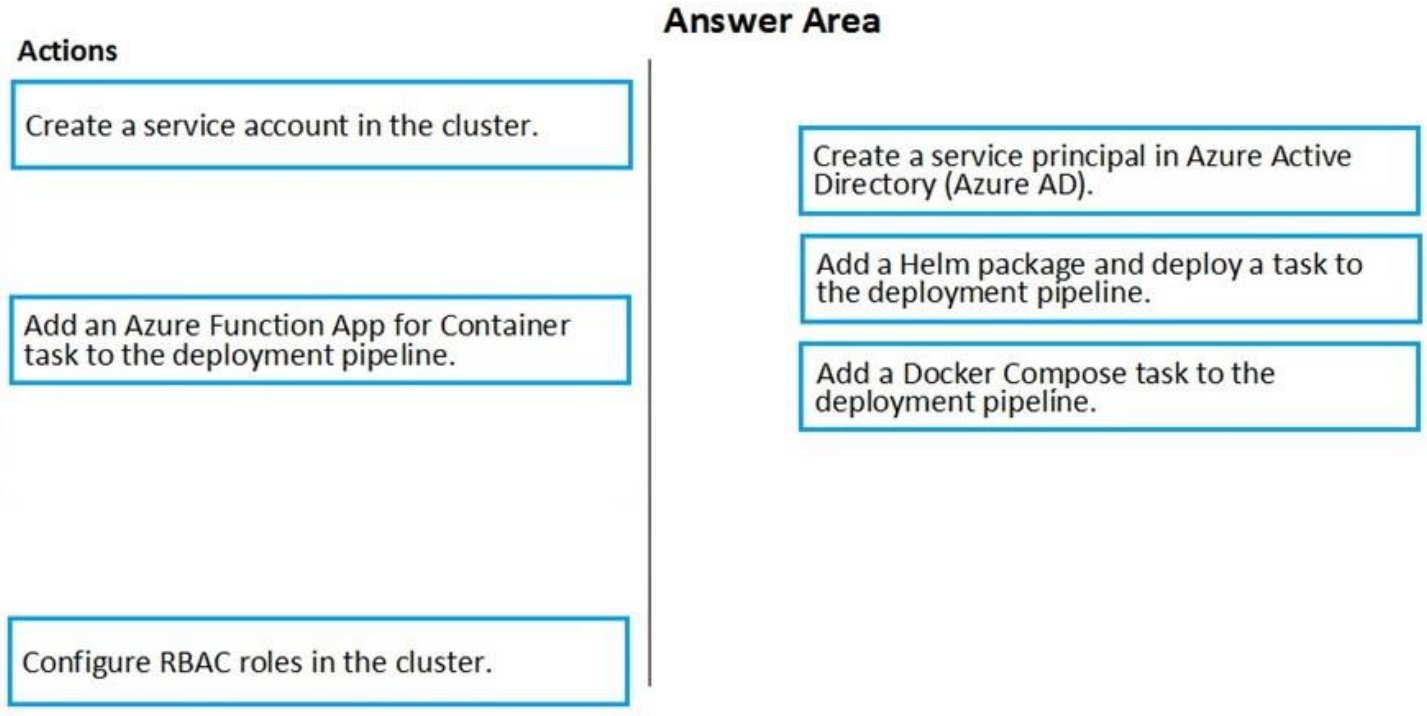
Explanation:
Box 1: Azure Container Registry
Azure services like Azure Container Registry (ACR) and Azure Container Instances (ACI) can be used and connected from independent container orchestrators like kubernetes (k8s). You can set up a custom ACR and connect it to an existing k8s cluster to ensure 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

Q157. 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.



A. Create a service account in the cluster
B. Create a service principal in Azure Active Directory (Azure AD)1
C. Add an Azure Function App for Container task to the deployment pipeline
D. Add a Helm package and deploy a task to the deployment pipeline2
E. Add a Docker Compose task to the deployment pipeline3
F. Configure RBAC roles in the cluster

Answer: BDE



Explanation:

You can set up a CI/CD pipeline to deploy your apps on a Kubernetes cluster with Azure DevOpsby 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 DevOpsworkflow 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-cicdpipeline-kuberneteshttps://cloudblogs.microsoft.com/opensource/2018/11/27/tutorial-azure-devops-setup-cicdpipeline-kubernetes-docker-helm/docker-helm/

Q158. 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

Q159. 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

Q160. 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

Q161. 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: D

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

Q162. 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

Q163. During a code review, you discover many quality issues. Many modules contain unused variables and empty catch blocks.
You need to recommend a solution to improve the quality of the code.
What should you recommend?

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

Answer: B

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 xcodebuild.
Reference: https://pmd.github.io/

Q164. 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://azuredevopslabs.com/labs/azuredevops/agile/

Q165. 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
E. NUnit
F. Coverage.py

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.
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

Q166. 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

Q167. 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

Q168. 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

Q169. 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 enforceyour team's code Quality and change management standards.
Reference: https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

Q170. 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: B

Explanation:
WhiteSource is the leader in continuous open source software security and compliance management.
WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and Quality of your open source components against WhiteSource constantly- updated definitive database of open source repositories.
Reference: https://azuredevopslabs.com/labs/vstsextend/whitesource/

Q171. 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/

Q172. You plan to update the Azure DevOps strategy of your company. You need to identify the following issues as they occur during the company's development process:

- *Licensing violations*
- *Prohibited libraries*

Solution: You implement automated security testing.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use implement continuous integration.
Note: WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and Quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.
Reference: https://azuredevopslabs.com/labs/vstsextend/whitesource/

Q173. 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: B

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

Q174. 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: A

Explanation:
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

Q175. 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

Q176. 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

Q177. 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: A

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

Q178. You plan to use Terraform to deploy an Azure resource group.
You need to install the Required frameworks to support the planned deployment. Which two frameworks should you install? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: BD

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

Q179. 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?

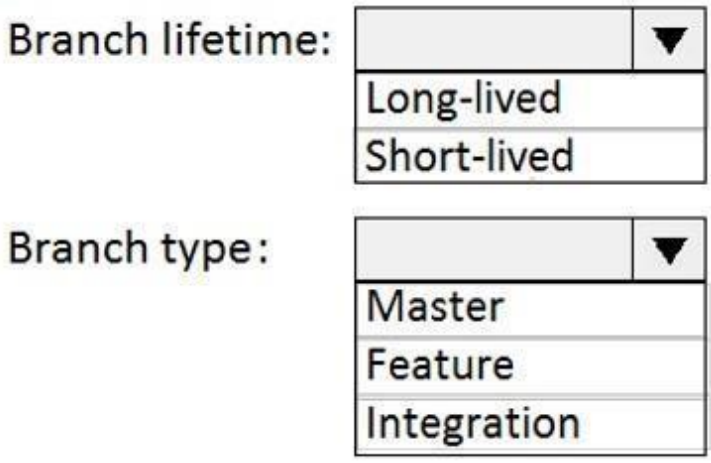
A. NuGet
B. Maven
C. Black Duck
D. Helm

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

Q180. 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.

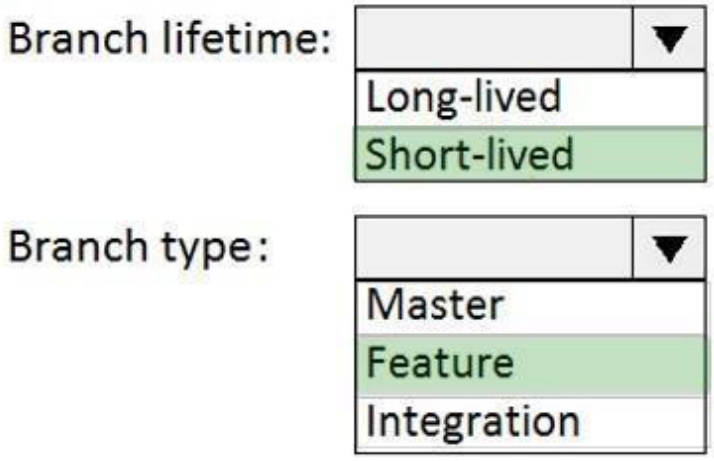
Answer Area



Box1
A. Long-lived
B. Short-lived
Box2
C. Master
D. Feature
E. Integration

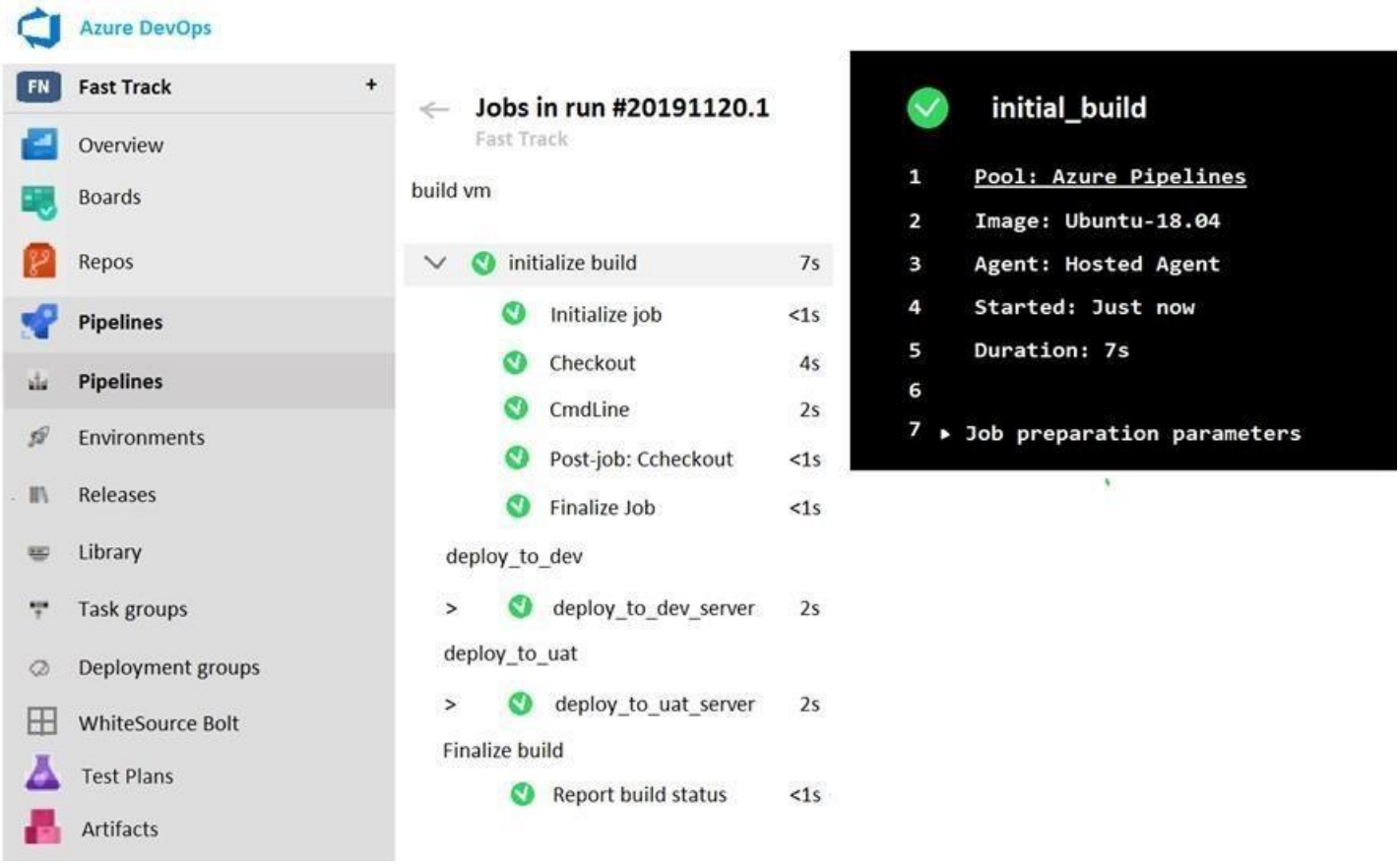
Answer: BD

Answer Area



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

Q181. 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.



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

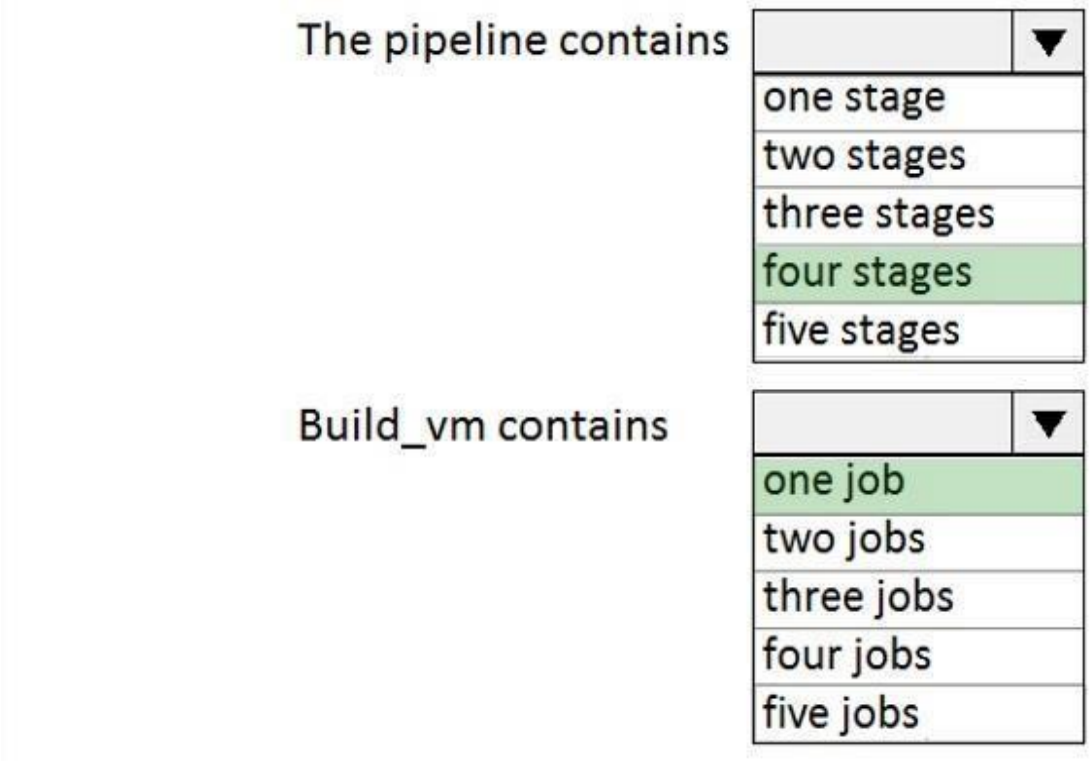
Build_vm contains

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

Box1
A. one stage
B. two stages
C. three stages
D. four stages
E. five stages
Box2
F. one job
G. two jobs
H. three jobs
I. four jobs
J. five jobs

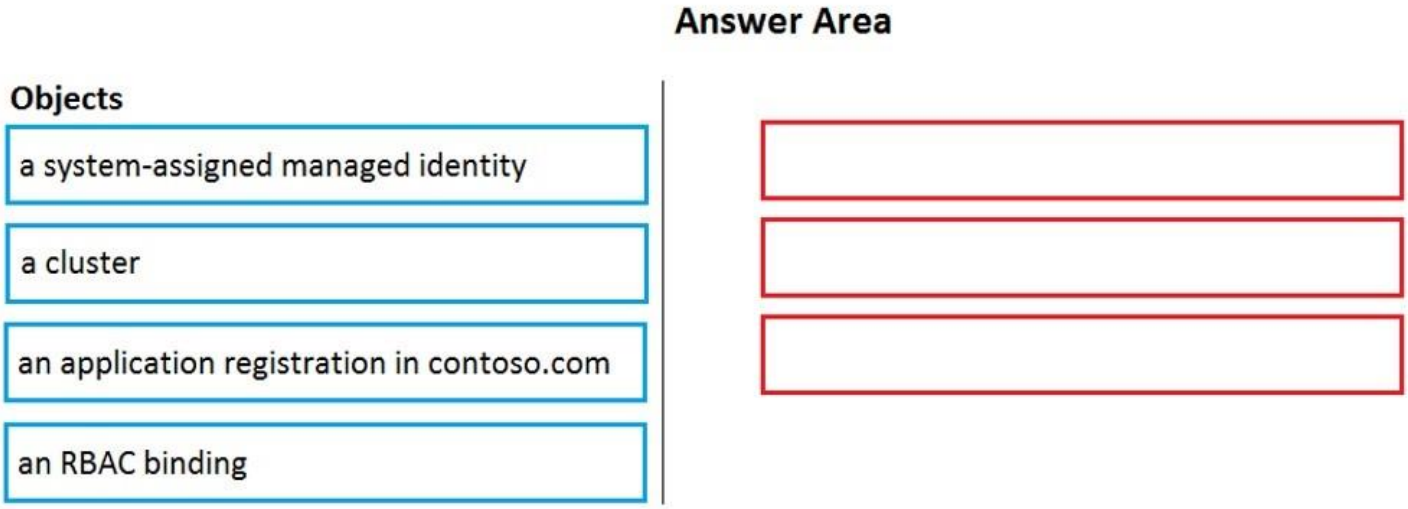
Answer: DF

Answer Area



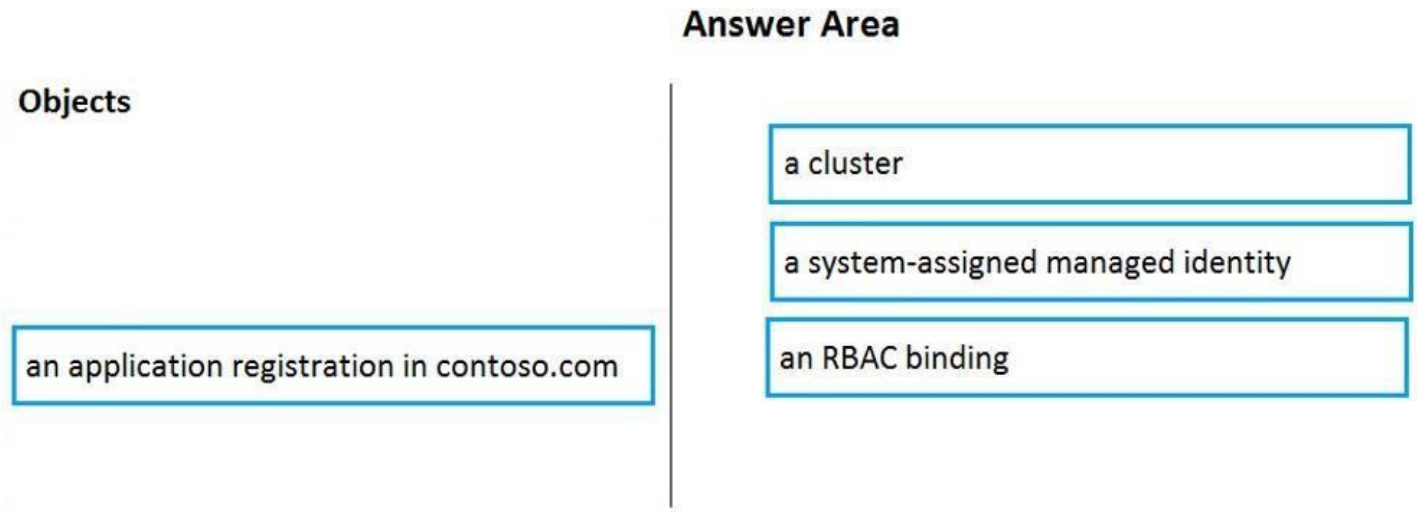
Explanation: https://dev.to/rajikaimal/azure-devops-ci-cd-yaml-pipeline-4glj

Q182. 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.

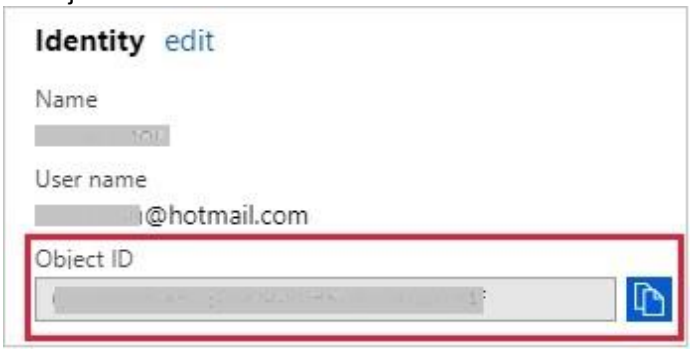


A. a system-assigned managed identity.[2]
B. a cluster[1]
C. an application registration in contoso.com
D. an RBAC binding[3]

Answer: BAD



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.



Step 3: a RBAC binding
Reference: https://docs.microsoft.com/en-us/azure/developer/ansible/aks-configure-rbac

Q183. 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:
- 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

Box1
A. Azure Resource Manager
B. Generic Service
C. Team Foundation Server / Azure Pipelines service connection
Box2
D. Azure Active Directory OAuth 2.0
E. Grant Authorization
F. Managed Service Identity Authentication

Answer: CF

Answer Area

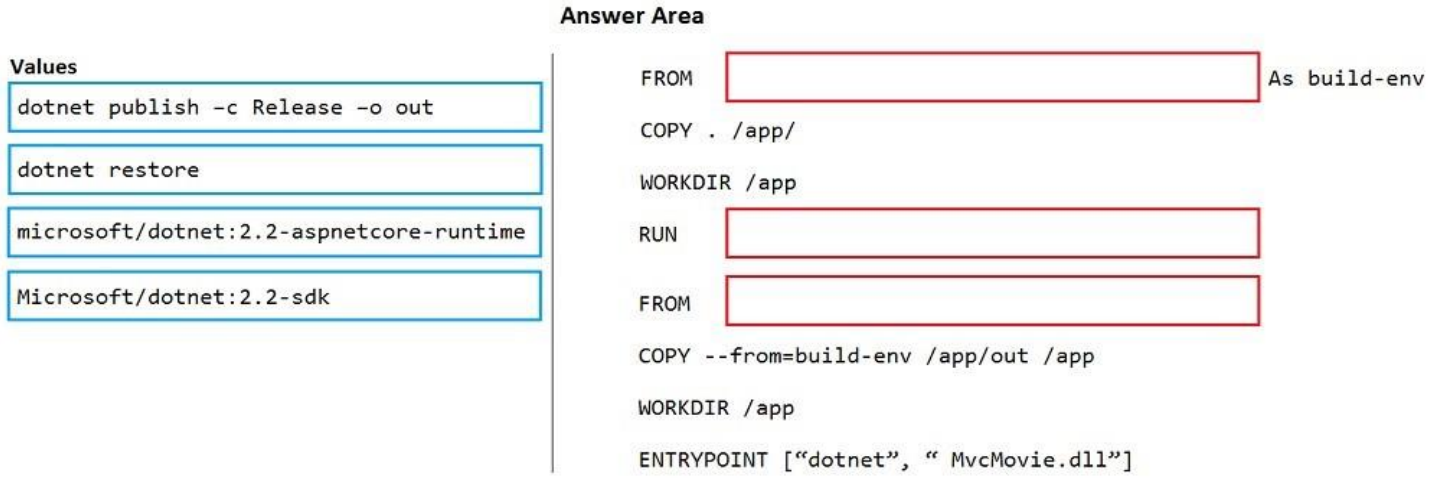
Service connection type:
- Azure Resource Manager
- Generic service
- Team Foundation Server / Azure Pipelines service connection

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-azureresources/overview

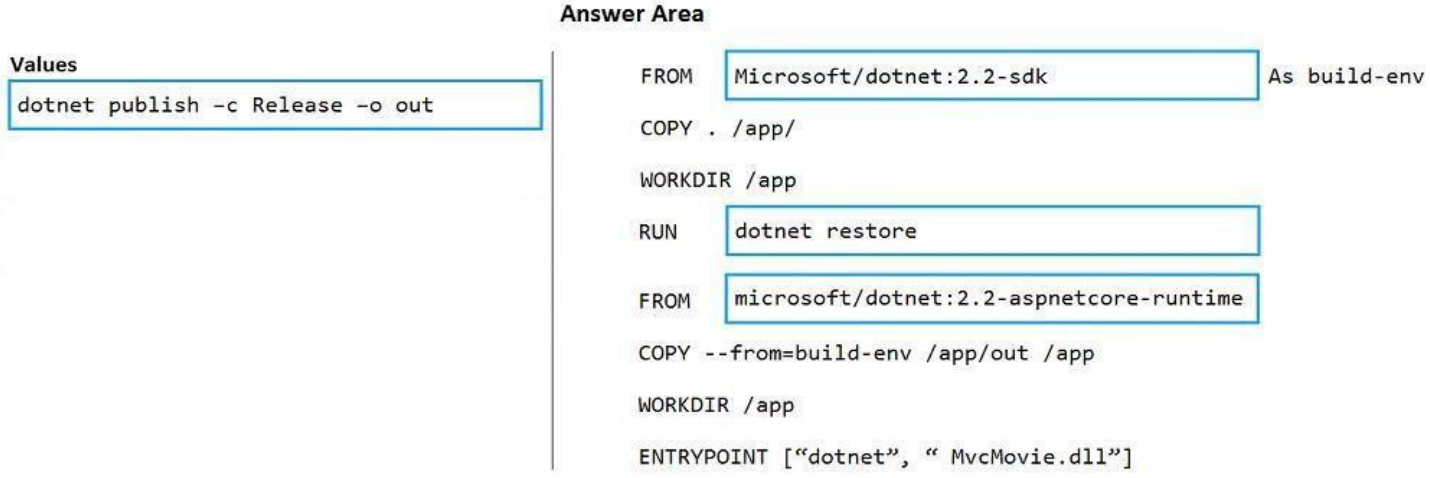
Q184. Drag and Drop question
You are creating a container for an ASP.NET Core app.
You need to create a Dockerfile file to build the image. The solution must ensure that the size of the image is minimized.
How should you configure the file? To answer, drag the appropriate values to the correct targets.

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.



A. dotnet publish –c Release –o out
B. dotnet restore[2]
C. Microsoft/dotnet:2.2-aspnetcore-runtime[3]
D. Microsoft/dotnet:2.2-sdk[1]

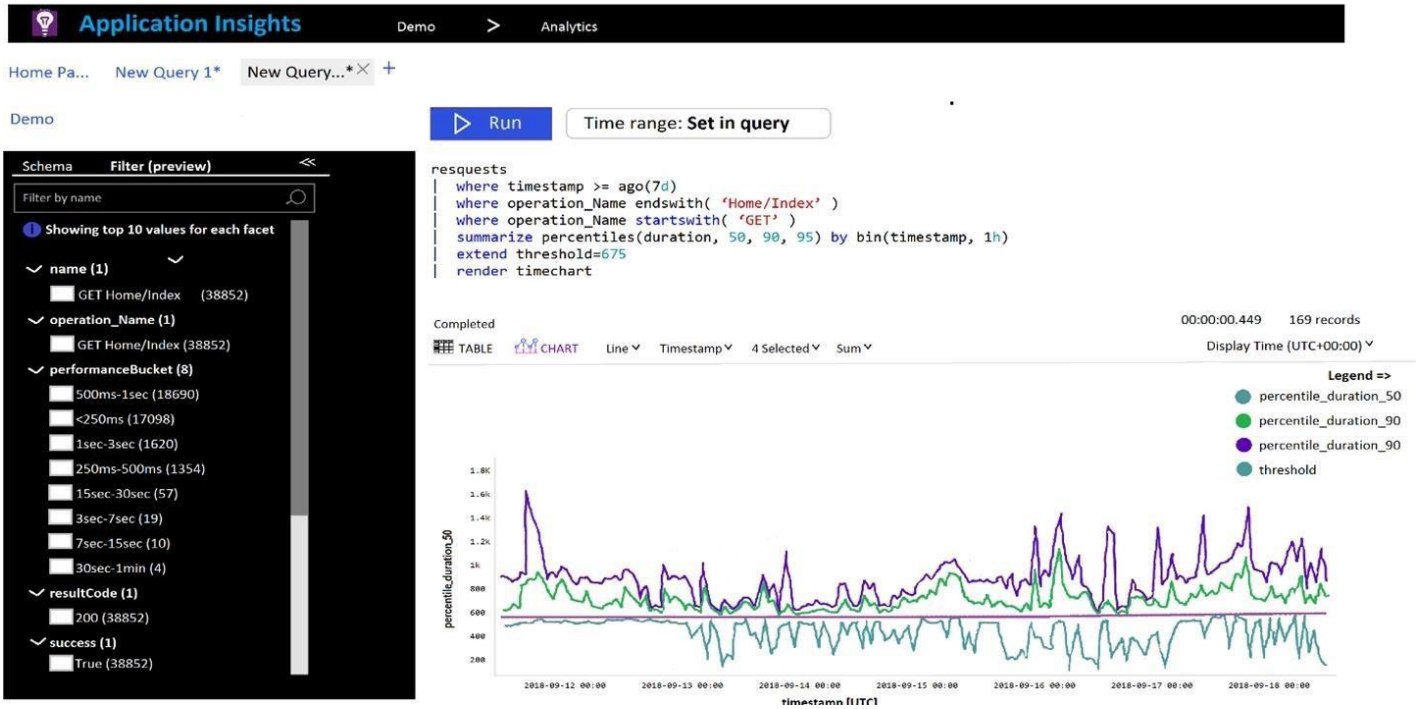
Answer: DBC



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 cr.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-sampleapp

Q185. 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]**.

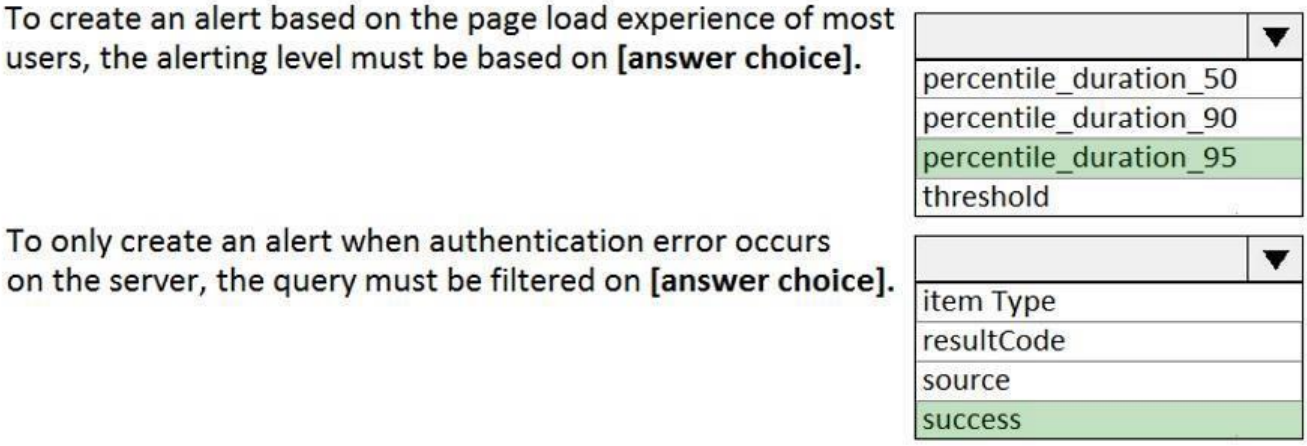
- item Type
- resultCode
- source
- success

Box1
A. percentile_duration_50

B. percentile_duration_90
C. percentile_duration_95
D. threshold
Box2
E. item Type
F. resultCode
G. source
H. success

Answer: CH

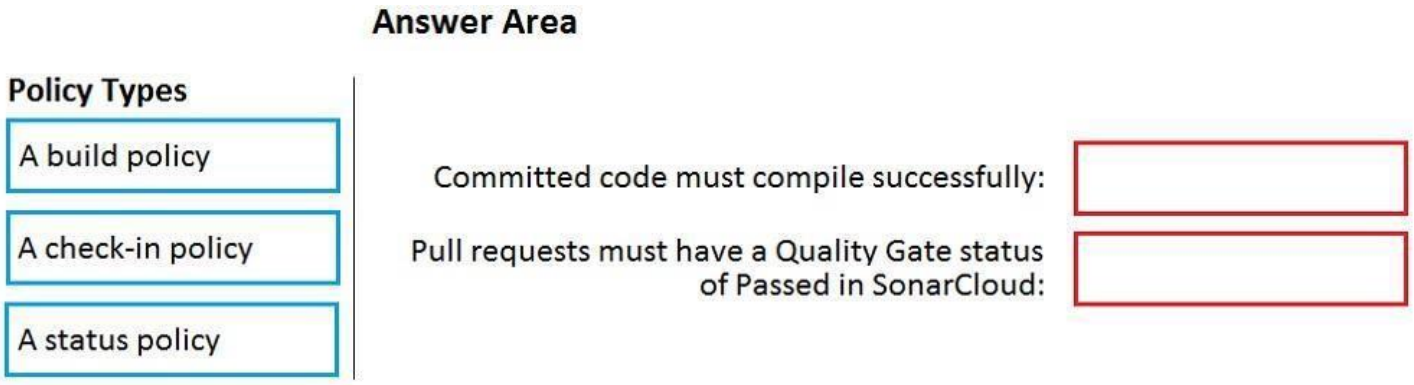
Answer Area



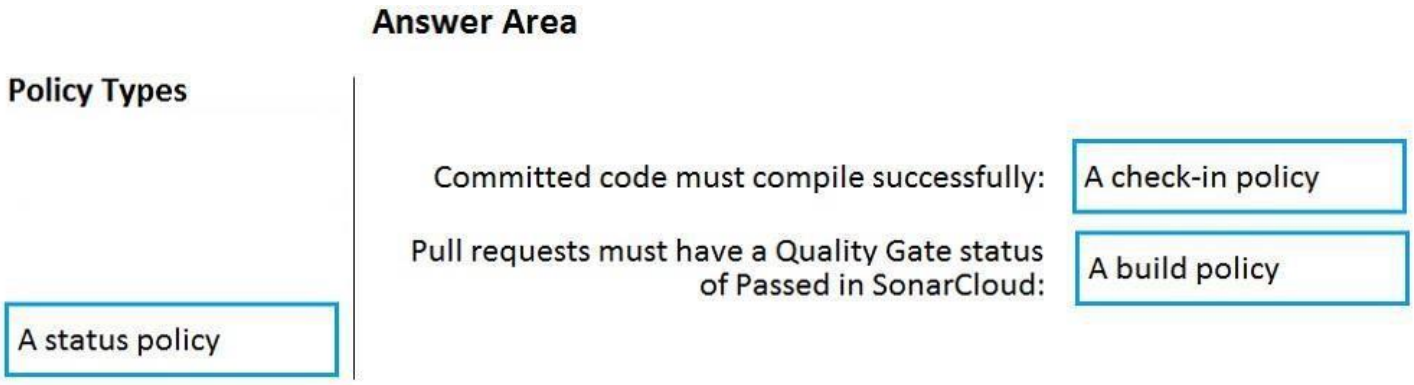
Explanation:
Box 1: percentile_duration_95
Box 2: success For example – requests
| project name, url, success
| where success == "False"
This will return all the failed requests in my App Insights within the specified time range.
Reference: https://devblogs.microsoft.com/premier-developer/alerts-based-on-analytics-Query-using-customlog-search/

Q186. 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.



A. A build policy[2]
B. A check-in policy[1]
C. A status policy
Answer: BA



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

Q187. Case Study 1 - Litware
Overview
Existing Environment
Litware, Inc. e 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'
```

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

Box1
A. Certificate
B. Personal access token
C. Shared Access Authorization token
D. Username and password
Box2
E. Azure Data Lake
F. Azure Key vault
G. Azure Storage with HTTPS access
H. Azure Storage with HTTP access

Answer: CG

Answer Area

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

Q188. 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 Thirdparty application access via OAuth for the organization setting to On.
Reference: https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams

Q189. 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: CDE

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

Q190. 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

Q191. 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 Cherrypick.
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

Q192. 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: C

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

Q193. 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: C

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

Q194. 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/

Q195. Your company has an Azure DevOps project,
The source code for the project is stored in an on-premises repository and uses on an on-premises build server.
You plan to use Azure DevOps to control the build process on the build server by using a selfhosted 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: DE

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

Q196. 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: ACD

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

Q197. 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: D

Explanation:

Use Docker when running integration tests with Azure Pipelines.
References: https://crossprogramming.com/2019/12/27/use-docker-when-running-integration-tests-withhttps://crossprogramming.com/2019/12/27/use-docker-when-running-integration-tests-with-azurepipelines.htmlazurepipelines.html

Q198. 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

Q199. 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-imageupdate

Q200. 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: C

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

Q201. 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/

Q202. 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

Q203. 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: D

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

Q204. 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 many 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

Q205. 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: CE

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

Q206. 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: A

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

Q207. 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/

Q208. 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: C

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

Q209. 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: BD

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

Q210. 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-aurl-ping-test

Q211. 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.
Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview

Q212. 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: B

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

Q213. 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.

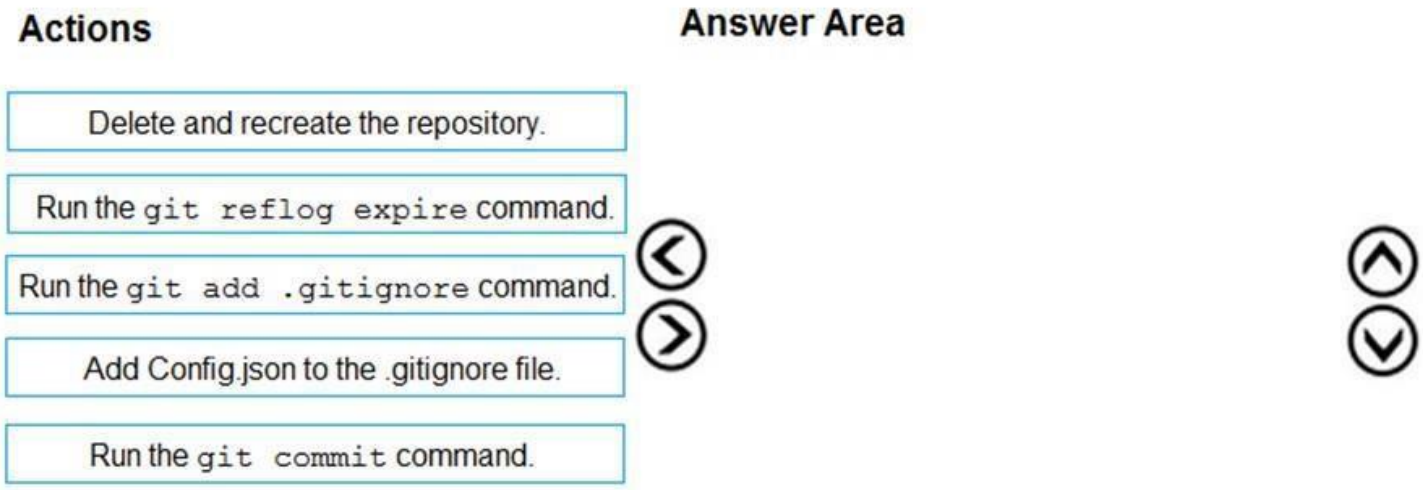
Answer: A

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

Q214. Drag and Drop question

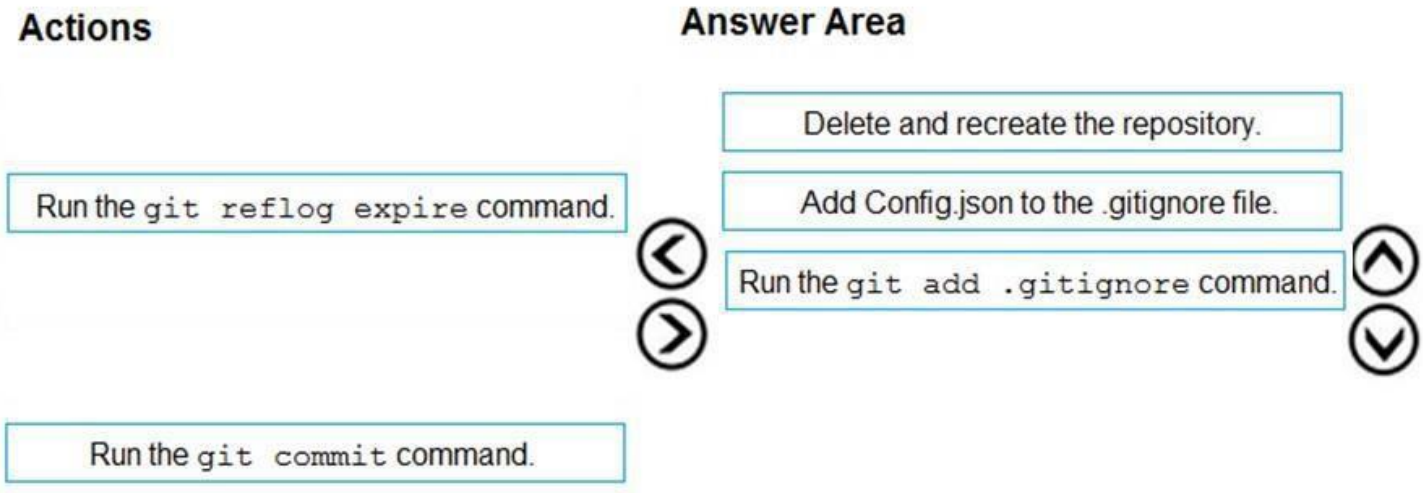
You manage the Git repository for a large enterprise application.
During the development of the application, you use a file named Config.json.

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.



A. Delete and create the repository[1]
B. Run the git reflog expire command
C. Run the git add .gitignore command[3]
D. Add Config.json to the .gitignore file[2]
E. Run the git commit command

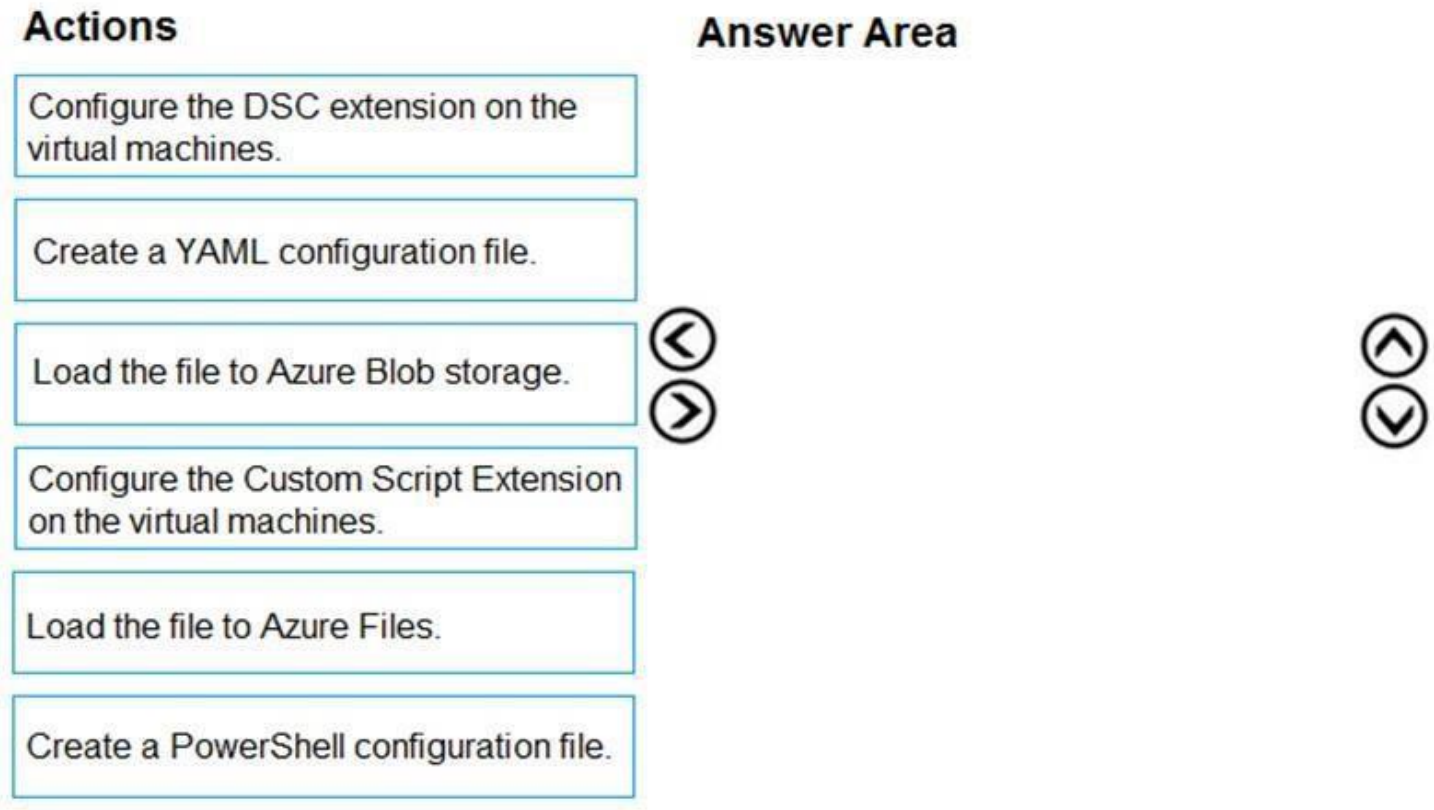
Answer: ADC



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

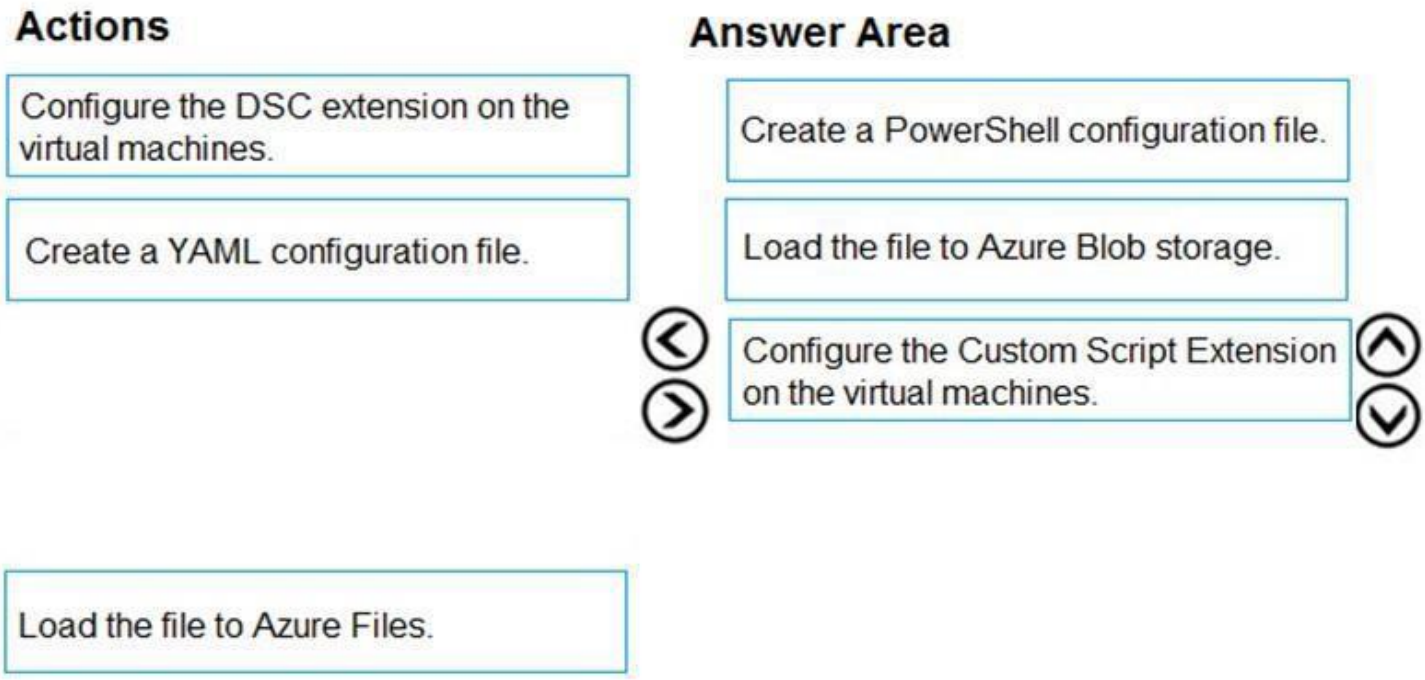
At the initial commit we want basically move from Untracked to Staged, for staging we have to indicate which file we want to move or specify a pattern, as example:
Reference: http://hermit.no/how-to-find-the-best-gitignore-for-visual-studio-and-azure-devops/
https://geohernandez.net/how-to-add-an-existing-repository-into-azure-devops-repo-with-git/

Q215. 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.



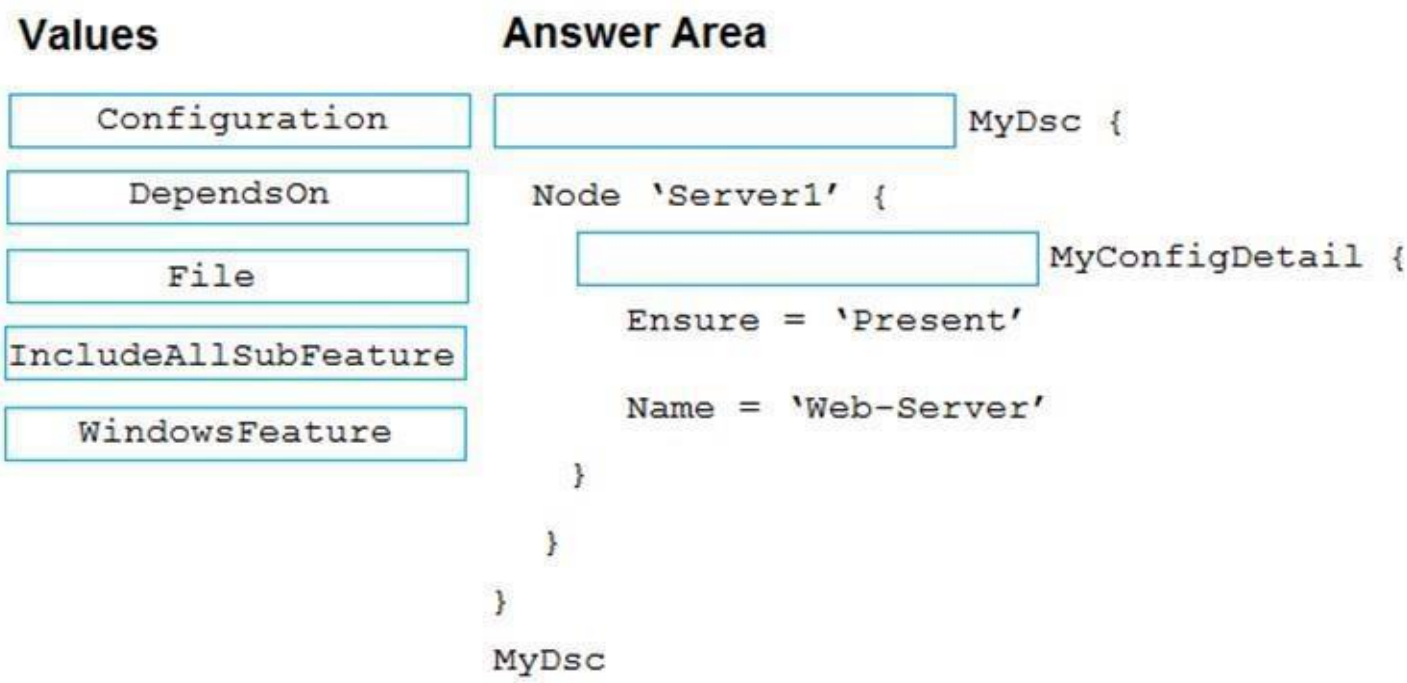
A. Configure the DSC extension on the virtual machine
B. Create a YAML configuration
C. Load the file to Azure Blob storage[2]
D. Configure the Custom Script Extension on the virtual machines[3]
E. Load the file to Azure Files
F. Create a PowerShell configuration file[1]

Answer: FCD



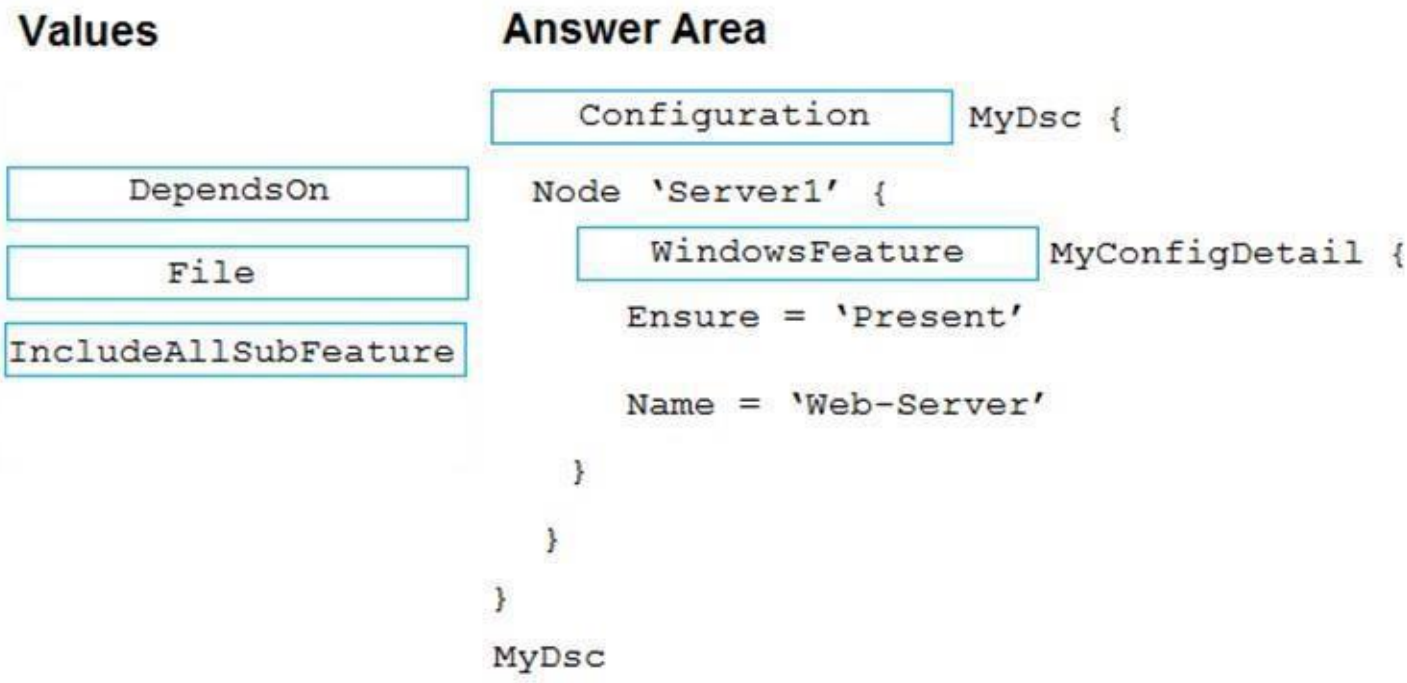
Explanation:
Step 1: Create a PowerShell configuration file
You create a simple PowerShell DSC configuration file.
Step 2: Load the file to Azure Blob storage
Package and publish the module to a publically accessible blob container URL
Step 3: Configure the Custom Script Extension on the virtual machines. 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

Q216. 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.



A. Configuration
B. DepenedsOn
C. File
D. IncludeAllSubFeature
E. WindowsFeature

Answer: AE



Explanation:
Box 1: Configuration
The following example shows a simple example of a configuration.
configuration IISInstall

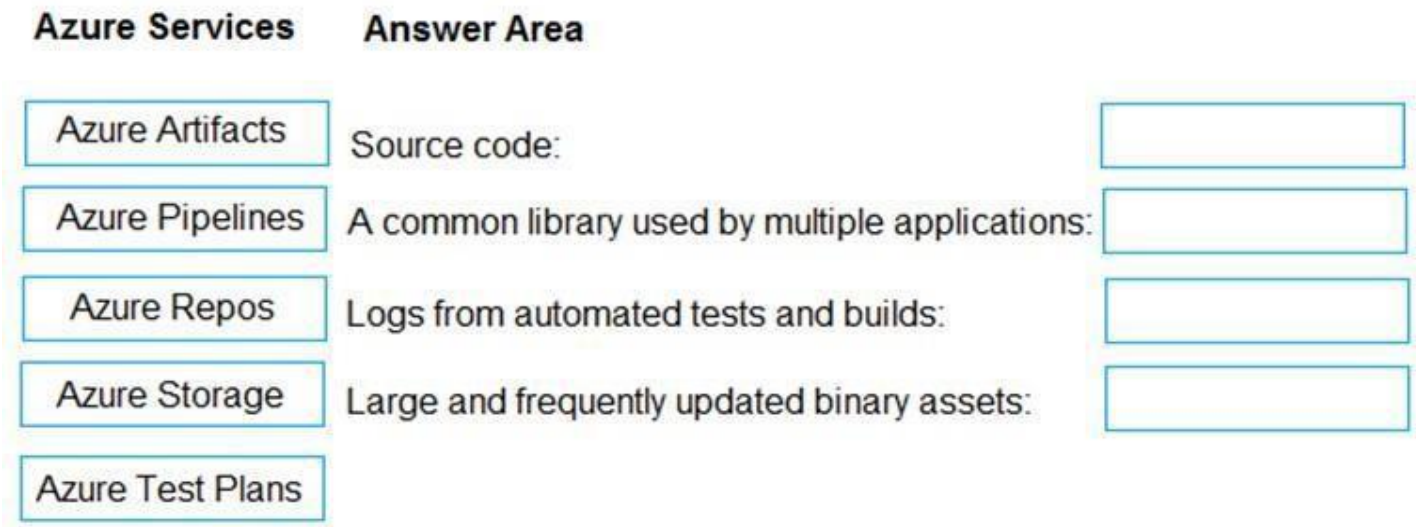
```
{
node "localhost"
{
WindowsFeature IIS
{
Ensure = "Present"
Name = "Web-Server"
}
}



}
```

Box 2: WindowsFeature
Reference: https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview

Q217. Drag and Drop question
You are building an application that has the following assets:

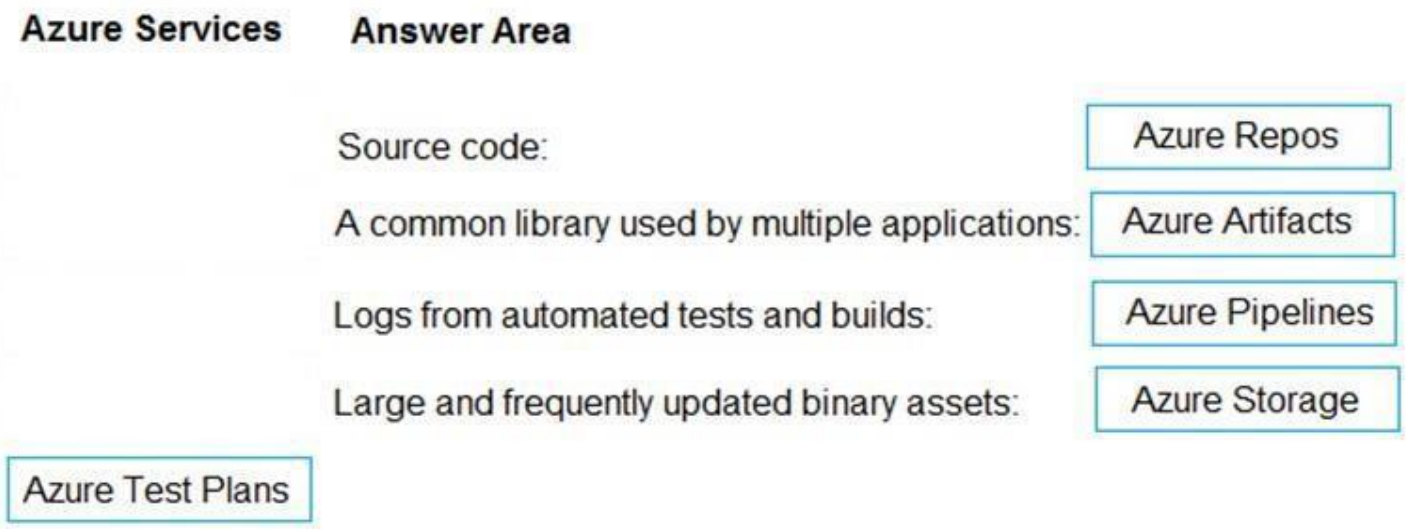
- *Source code*
- *Logs from automated tests and builds*
- *Large and frequently updated binary assets*
- *A common library used by multiple applications*

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.



A. Azure Artifacts[2]
B. Azure Pipelines[3]
C. Azure Repos[1]
D. Azure Storage[4]
E. Azure Test Plans

Answer: CABD

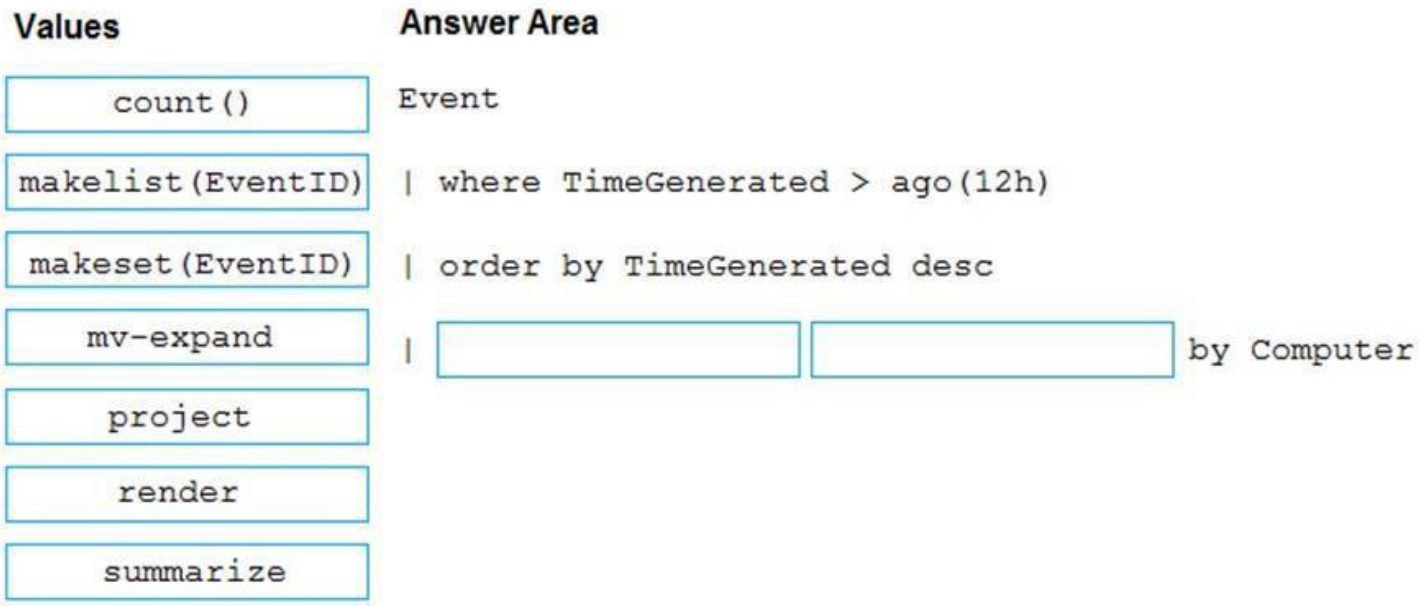


Explanation:
Box 1: Azure Repos
Box 2: Azure Artifacts
Use Azure Artifacts to create, host, and share packages with your team.
Box 3: Azure Pipelines
In the pipeline view you can see all the stages and associated tests. The view provides a summary of the test results Box 4: Azure Storage
Reference: https://docs.microsoft.com/en-us/azure/devops/repos/get-started/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-afterbuild

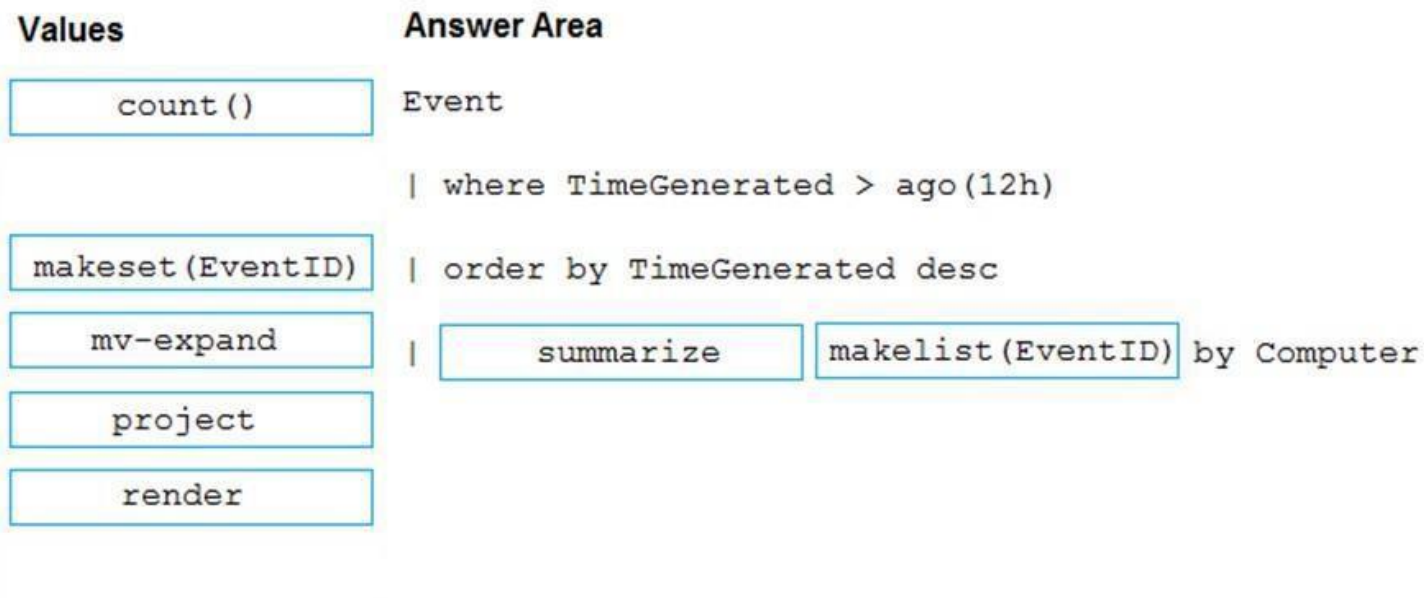
Q218. Drag and Drop question
You have several Azure virtual machines that run Windows Server 2019.
You need to identify the distinct event IDs of each virtual machine as shown in the following table.

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.



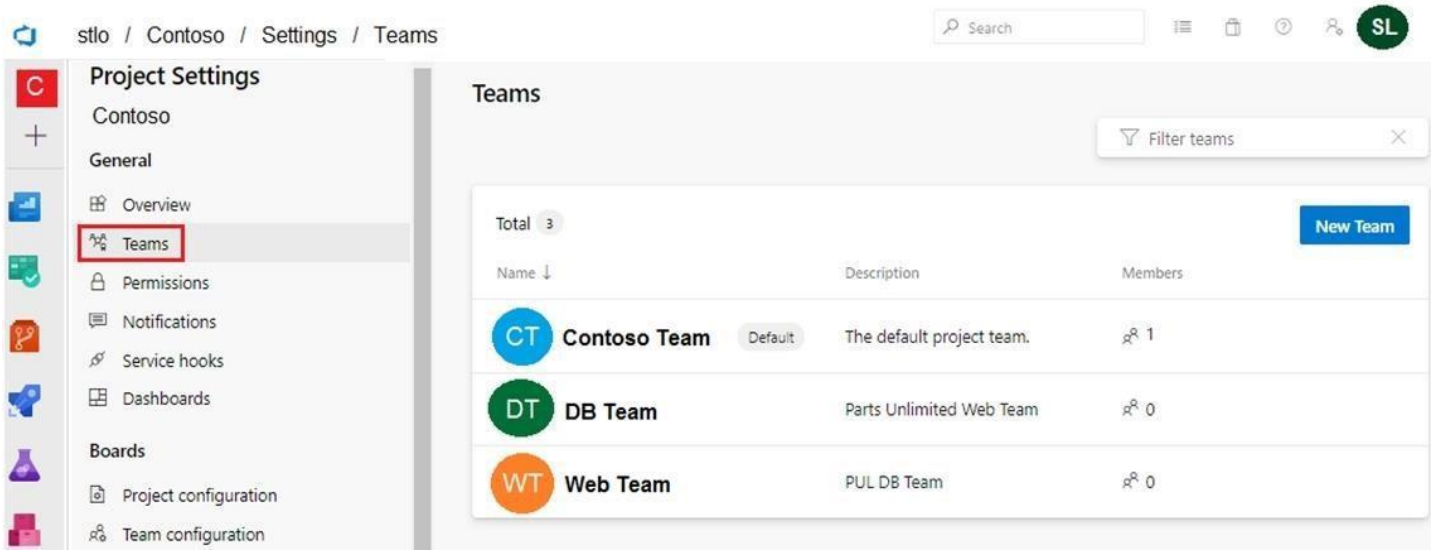
A. count ()
B. makelist (Event ID)[2]
C. makeset (Event ID)
D. mv-expand
E. project
F. render
G. summarize[1]
Answer: GB



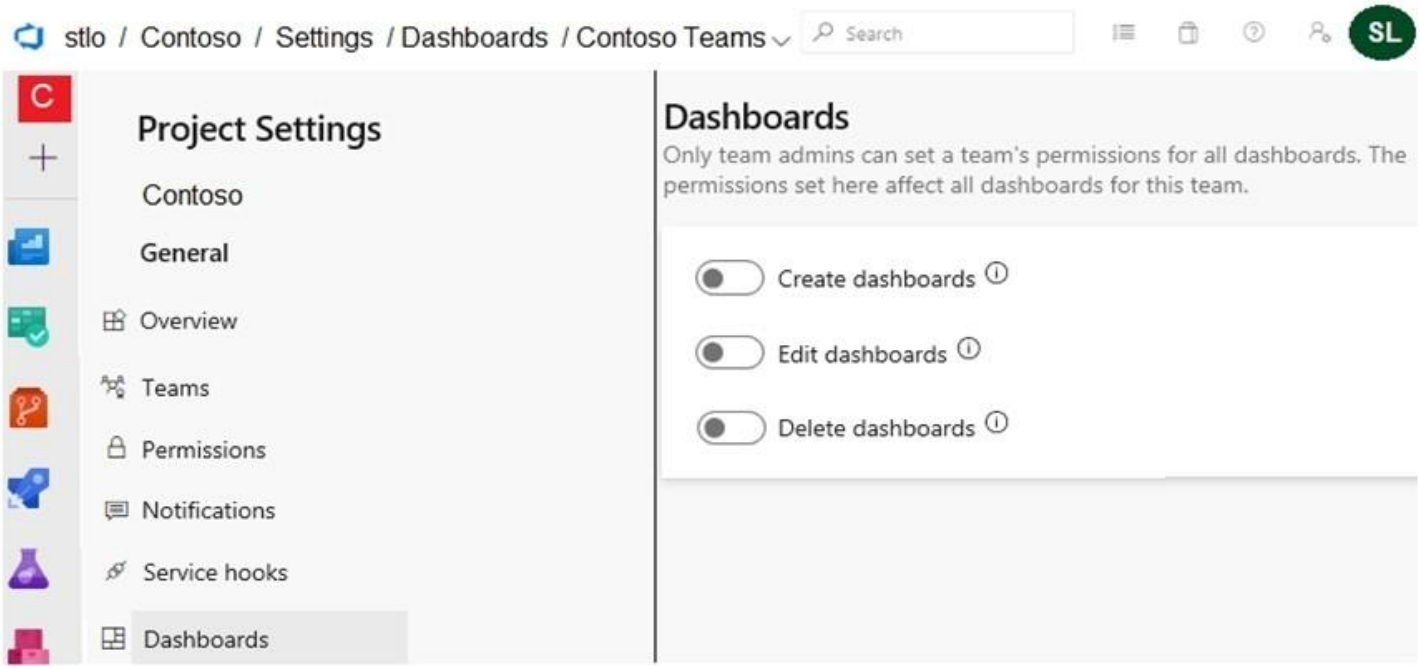
Explanation:
You can use makelist to pivot data by the order of values in a particular column. For example, you may want to explore the most common order events take place on your machines. You can essentially pivot the data by the order of EventIDs on each machine.
Example:
Event
| where TimeGenerated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

Q219. Hotspot question
You have a project in Azure DevOps that has three teams as shown in the Teams exhibit. (Click the Teams tab.)



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.)



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.	○	○
Contoso Team can view Dash1.	○	○
Project administrators can create new dashboards.	○	○

A. YYY
B. NNN
C. YNY
D. NYN
E. YYN
F. NNY
G. NYY
H. YNN

Answer: G

Answer Area

Statements	Yes	No
Web Team can delete Dash1.	○	○
Contoso Team can view Dash1.	○	○
Project administrators can create new dashboards.	○	○

Explanation: https://docs.microsoft.com/en-us/azure/devops/report/dashboards/charts-dashboard-permissionsaccess

Q220. 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

Q221. 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

Q222.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-forintegratinghttps://docs.microsoft.com/en-us/azure/active-directory/manage-apps/developer-guidance-forintegrating-applicationsapplications

Q223. 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

Q224. You have the following Azure policy.
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.

Q225. 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

Q226. 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: B

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

Q227. 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/

Q228. 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

Q229. 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

Q230. 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: B

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

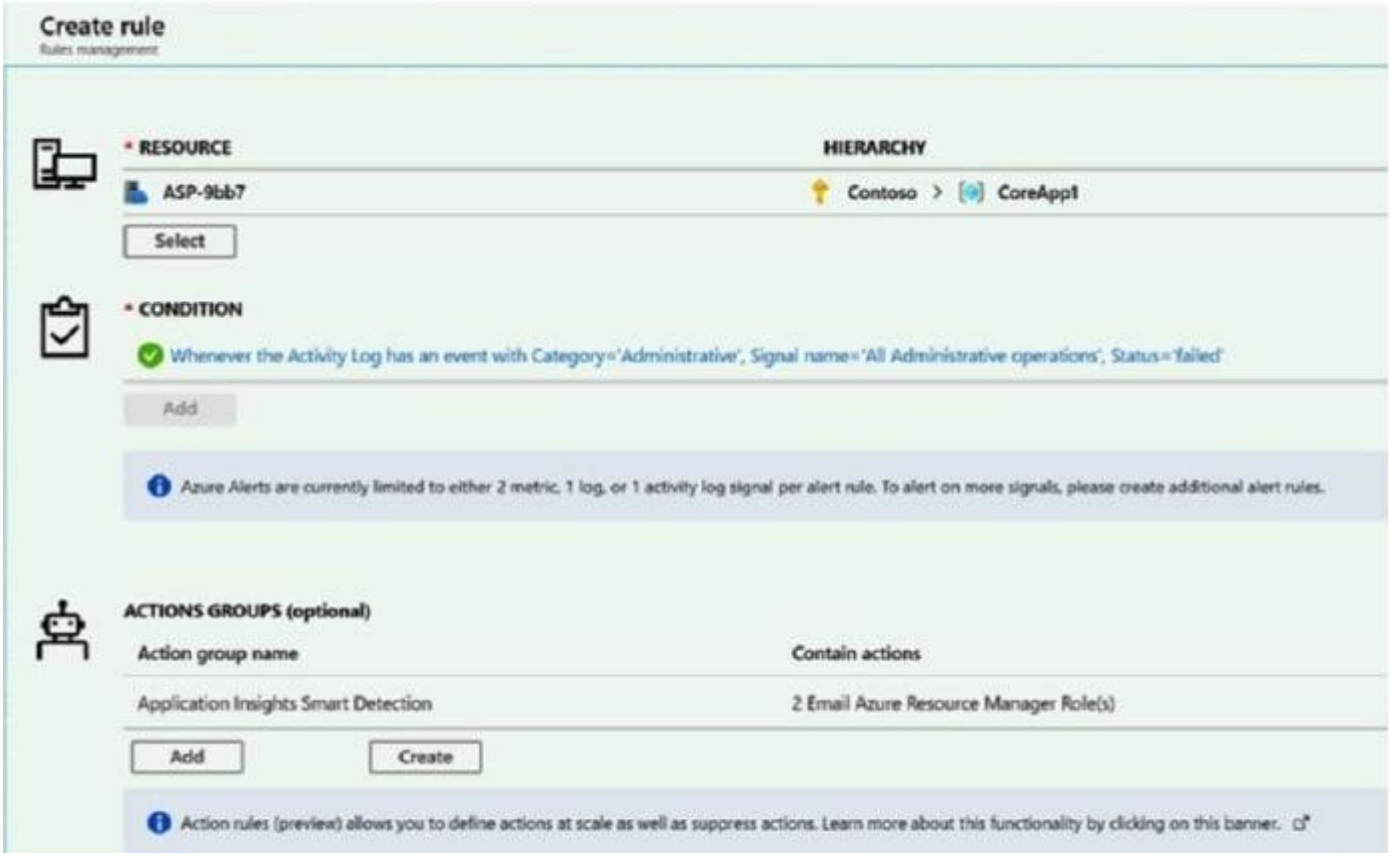
Q231. You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 that is configured for autoscaling.
You use Azure DevOps to build a web app named App1 and deploy App1 to VMSS1. App1 is used heavily and has usage 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

Q232. You create an alert rule in Azure Monitor as shown in the following exhibit.



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

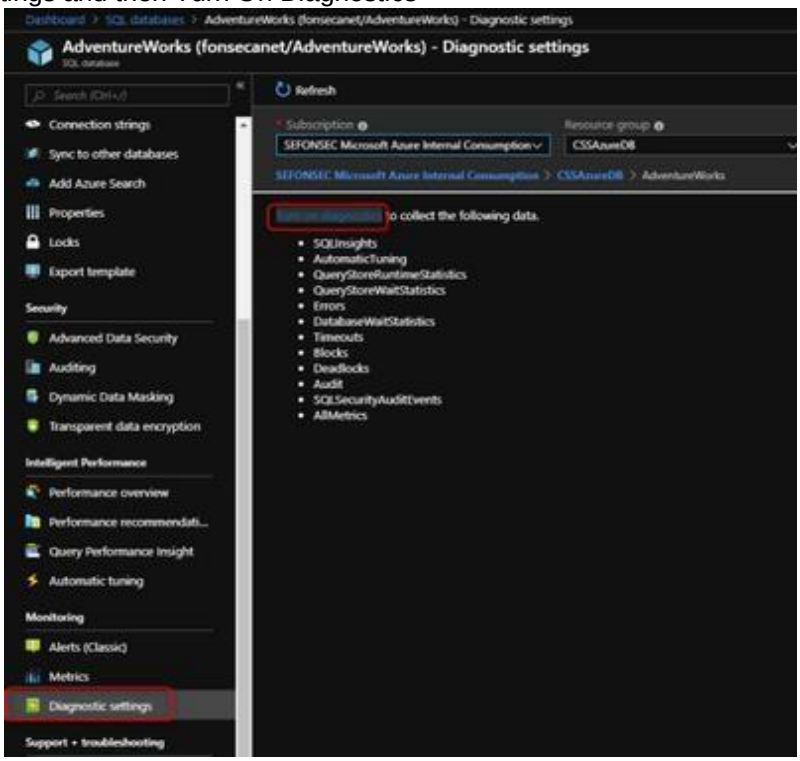
Answer: A

Q233. 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?

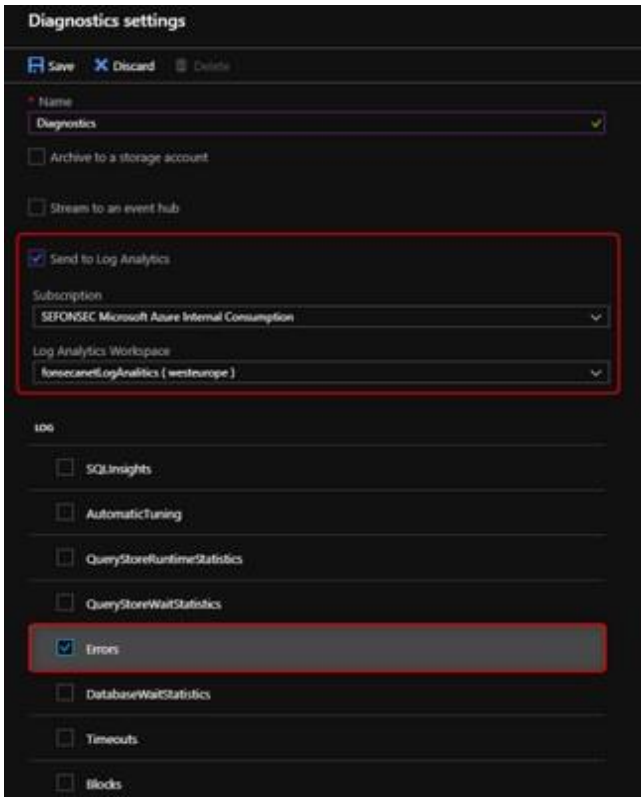
A. Send to Log Analytics
B. Stream to an event hub
C. Archive to a storage account

Answer: A

Explanation:
ENABLE DIAGNOSTICS TO LOG ANALYTICS
This configuration is done PER DATABASE
1. Click on Diagnostics Settings and then Turn On Diagnostics



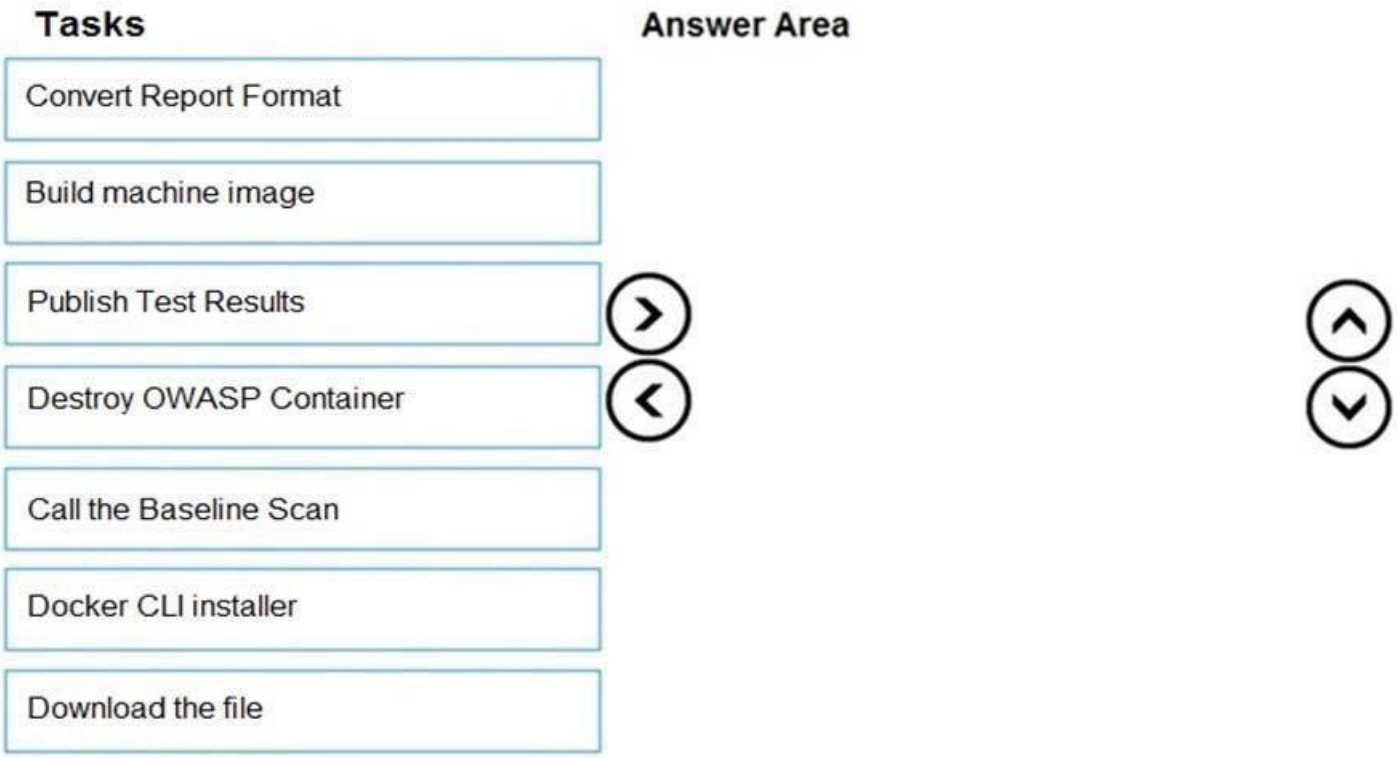
2. Select to Send to Log Analytics and select the Log Analytics workspace. For this sample I will selected only Errors



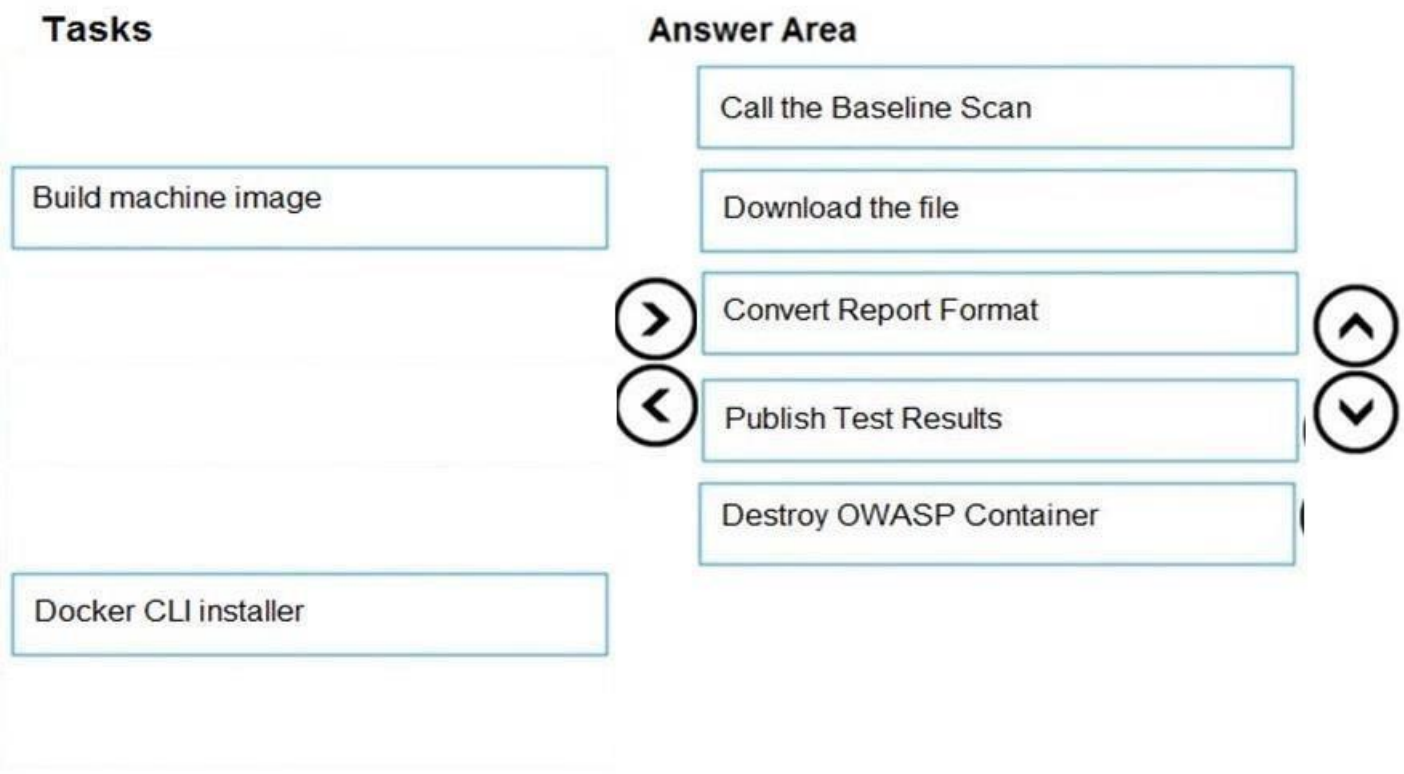
Reference: https://techcommunity.microsoft.com/t5/azure-database-support-blog/azure-sQl-db-and-loganalytics-betterhttps://techcommunity.microsoft.com/t5/azure-database-support-blog/azure-sQl-db-and-loganalytics-better-together-part-1/ba-p/794833together-part-1/ba-p/794833

Q234. Drag and Drop question
You have an Azure DevOps release pipeline as shown in the following exhibit.

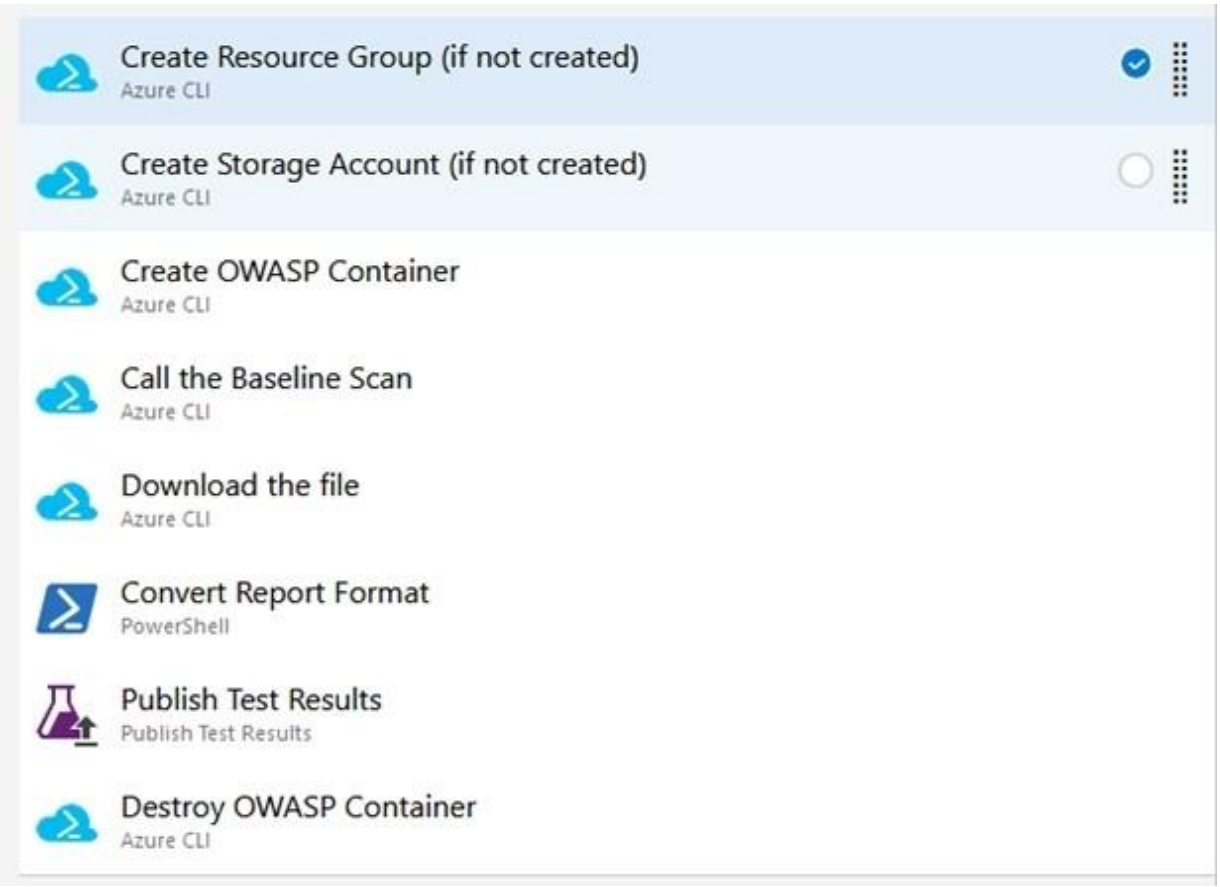
You need to complete the pipeline to configure OWASP ZAP for security testing.
Which five Azure CLI tasks should you add in sequence?
To answer, move the tasks from the list of tasks to the answer area and arrange them in the correct order.



A. Convert Report Format[3]
B. Build machine image
C. Publish Test Results[4]
D. Destroy OWASP Container[5]
E. Call the Baseline Scan[1]
F. Docker CLI installer
G. Download the file[2]
Answer: EGACD



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.



Reference: https://devblogs.microsoft.com/premier-developer/azure-devops-pipelines-leveraging-owasp-zapin-thehttps://devblogs.microsoft.com/premier-developer/azure-devops-pipelines-leveraging-owasp-zapin-the-release-pipeline/release-pipeline/

Q235. 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

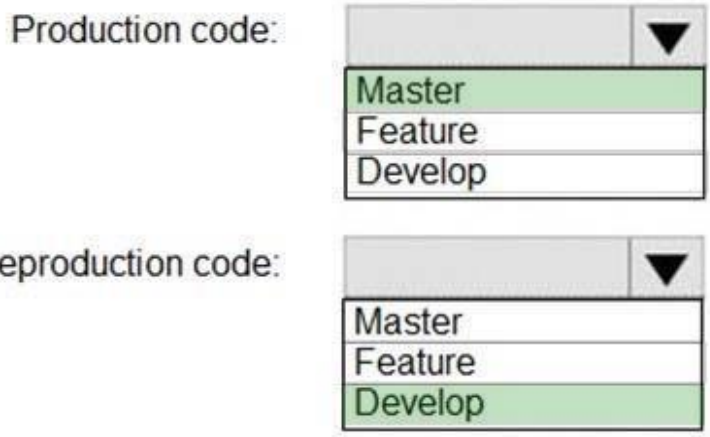
Production code:
- Master
- Feature
- Develop

Preproduction code:
- Master
- Feature
- Develop

Box1.
A. Master
B. Feature
C. Develop
Box2
D. Master
E. Feature
F. Develop

Answer: AF

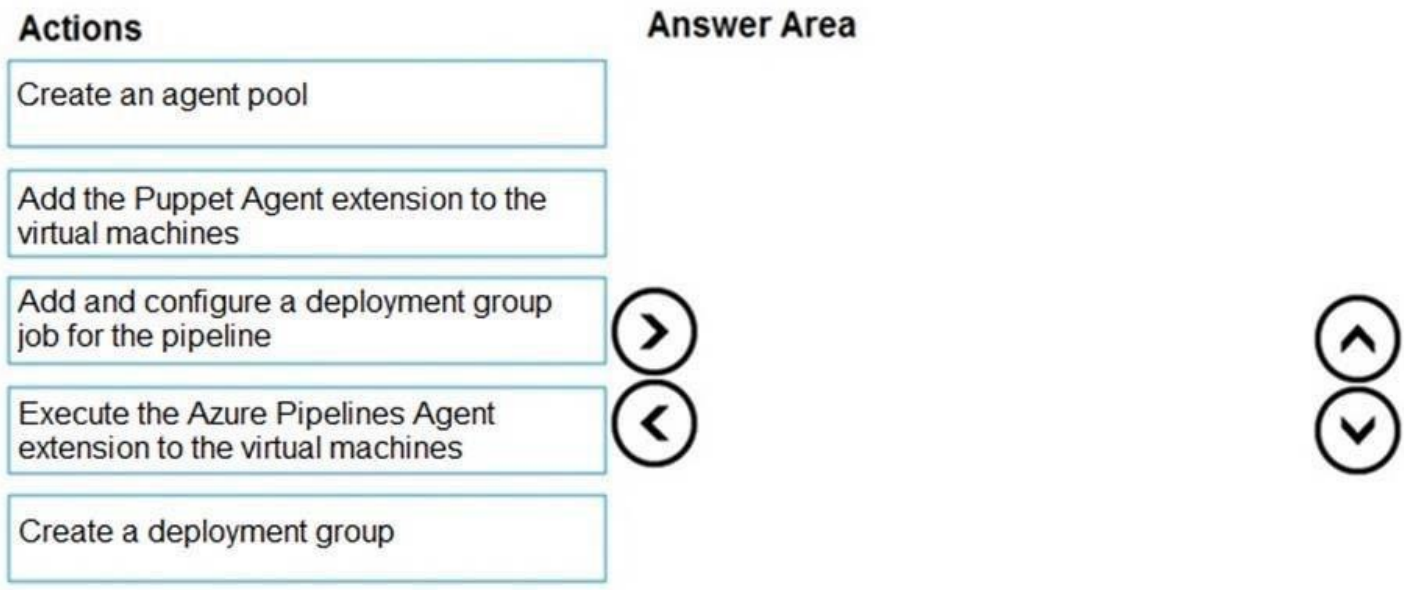
Answer Area



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

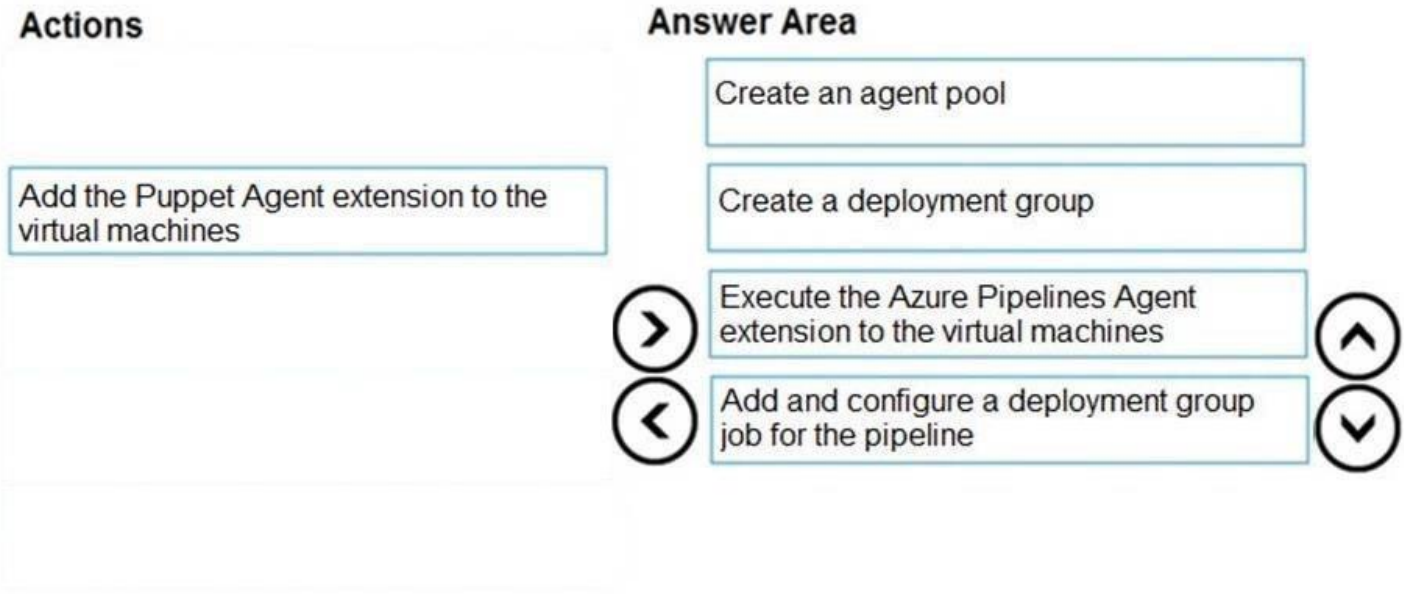
Q236. Drag and Drop question
You have an Azure subscription that contains a resources group named RG1. RG1 contains the following resources:
- *Four Azure virtual machines that run Windows Server and have Internet Services (IIS) installed.*
- *SQL Server on an Azure virtual machine.*
- *An Azure Load 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.



A. Create an agent pool[1]
B. Add the Puppet Agent extension to the virtual machines
C. Add and configure a deployment group job for the pipeline[4]
D. Execute the Azure Pipelines Agent extension to the virtual machines[3]
E. Create a deployment group[2]

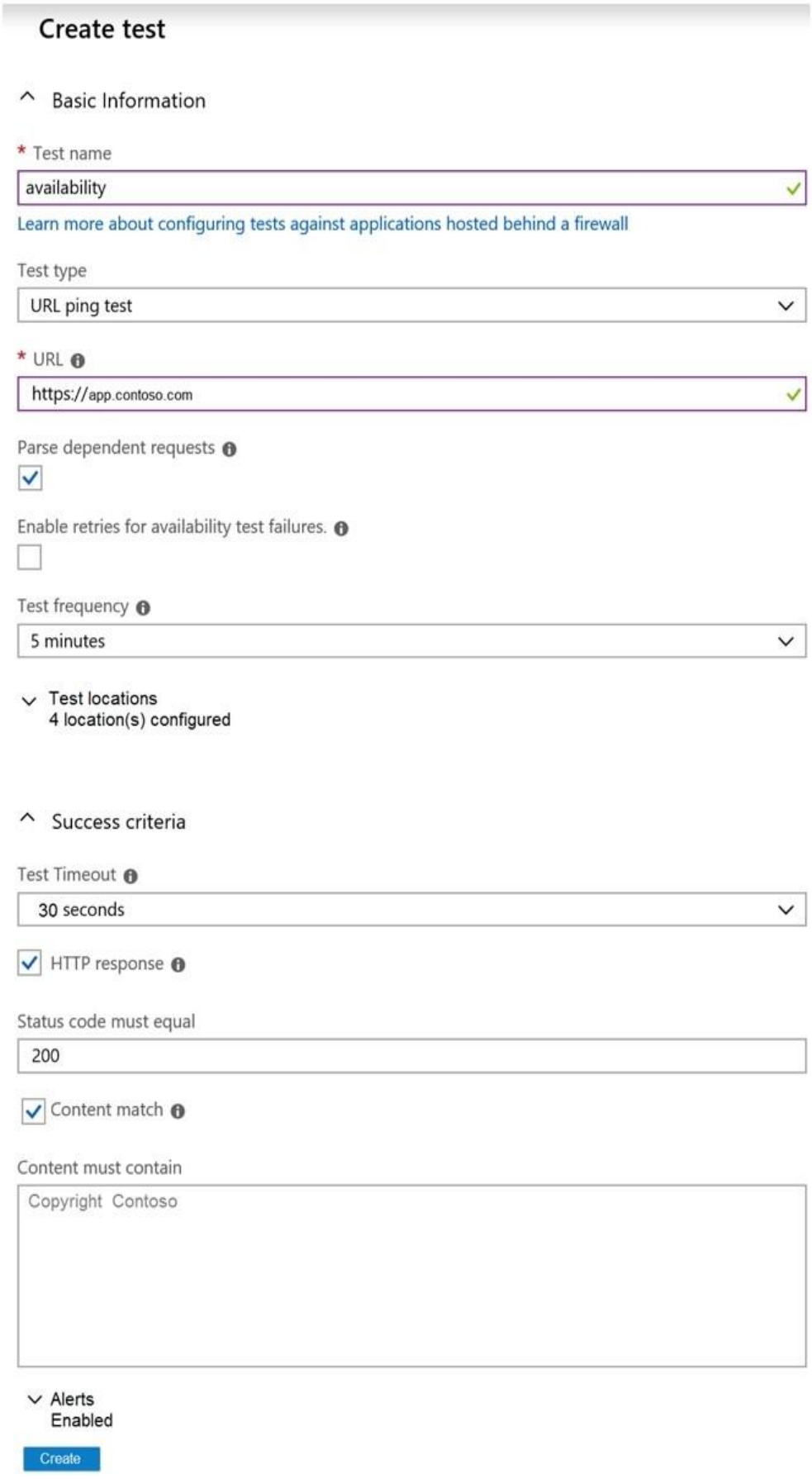
Answer: AEDC



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

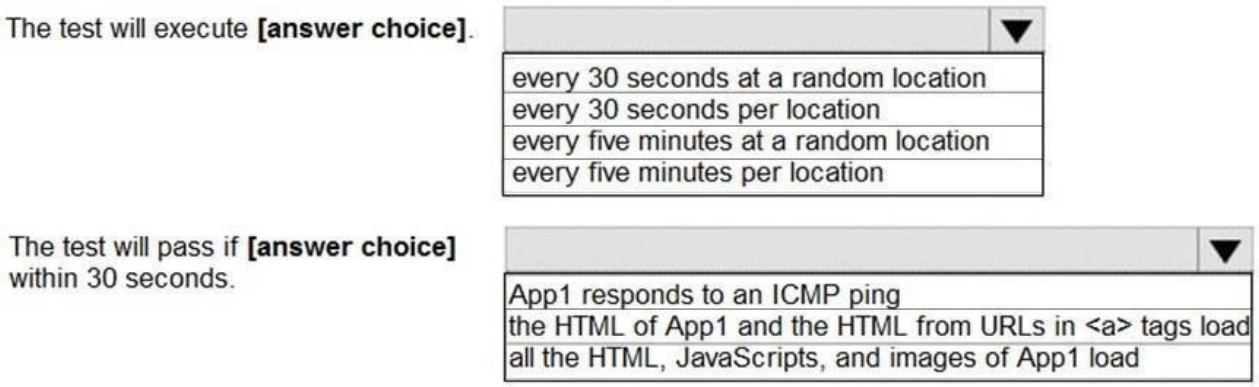
Pipelines Agent Azure VM extension
Step 4: Add and configure a deployment group job for the pipeline Tasks that you define in a deployment group job run on some or all of the target servers, depending on the arguments you specify for the tasks and the job itself. Reference: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deployment-groups/howtoprovision deployment-group-agents/

Q237. 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
availability
Learn more about configuring tests against applications hosted behind a firewall
Test type
URL ping test
* URL
https://app.contoso.com
Parse dependent requests
Enable retries for availability test failures.
Test frequency
5 minutes
Test locations
4 location(s) configured
Success criteria
Test Timeout
30 seconds
HTTP response
Status code must equal
200
Content match
Content must contain
Copyright Contoso
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.

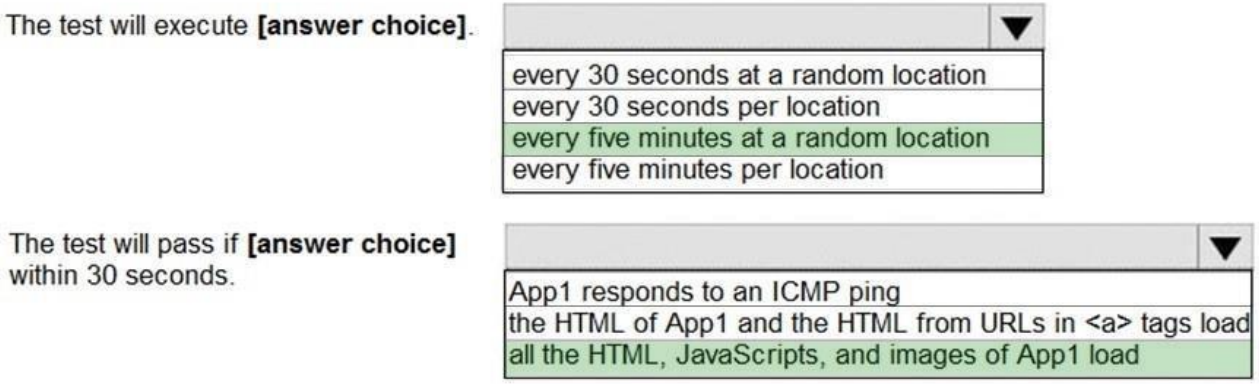
Answer Area



Box1
A. every 30 seconds at a random location
B. every 30 seconds per location
C. every five minutes at a random location
D. every five minutes per location
Box2
E. App1 responds to an ICMP ping
F. the HTML of App1 and the HTML from URLs in <a> tags load
G. all the HTML, JavaScripts, and images of App1 load

Answer: CG

Answer Area



Explanation:

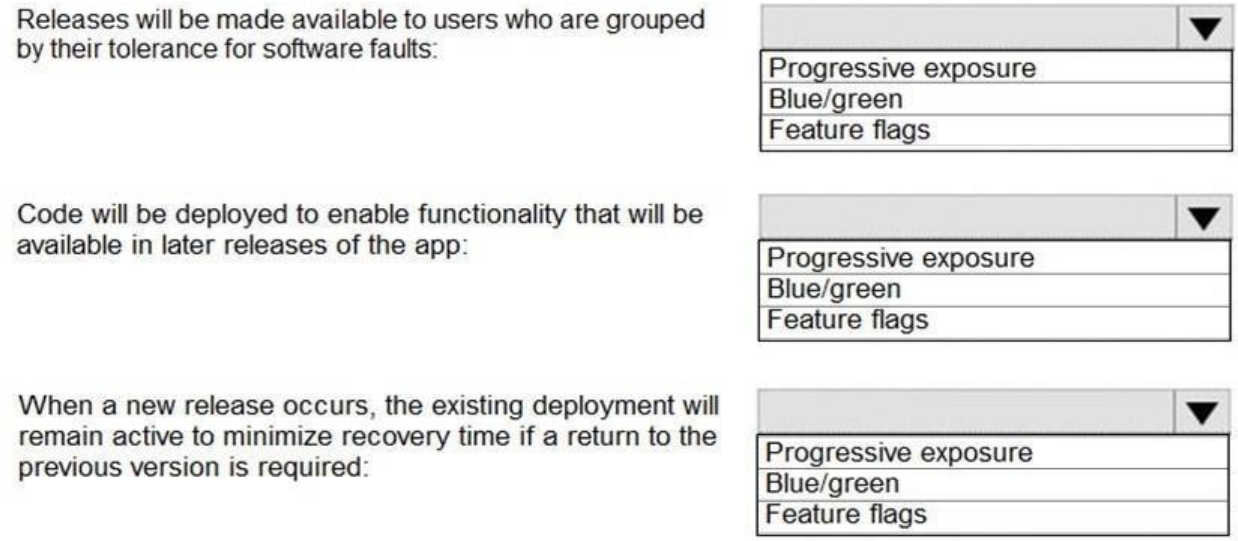
Box 1: every five minutes at a random location
Test frequency: Sets how often the test is run from each test location. With a default frequency of five minutes and five test locations, your site is tested on average every minute. Box 2:
Parse dependent requests: Test requests images, scripts, style files, 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

Q238. 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



Box1
A. Progressive exposure
B. Blue/green
C. Feature flags
Box2
D. Progressive exposure
E. Blue/green
F. Feature flags
Box3
G. Progressive exposure
H. Blue/green
I. Feature flags

Answer: AFH

Answer Area

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

- Progressive exposure
- Blue/green
- Feature flags

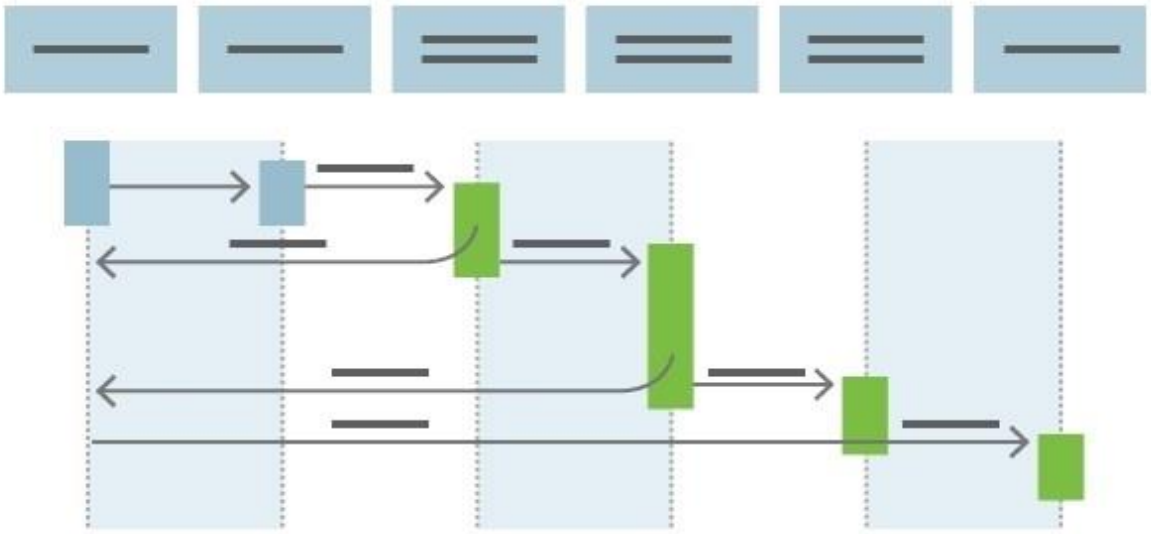
Code will be deployed to enable functionality that will be available in later releases of the app:

- 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

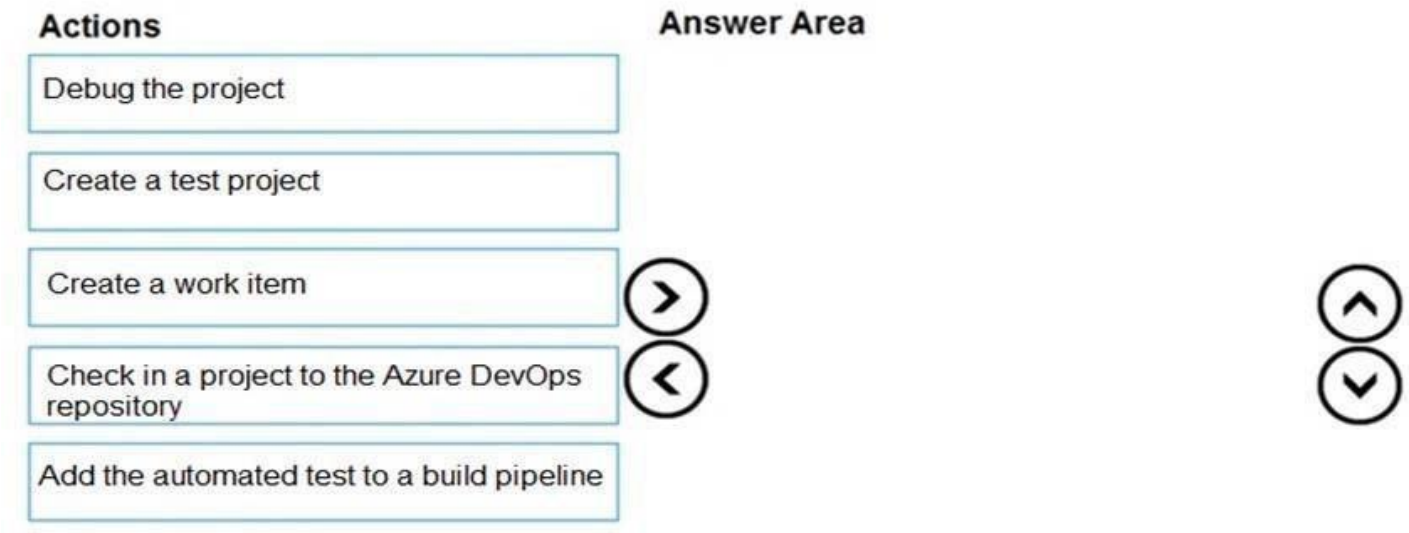
Explanation:
Box 1: Progressive exposure
Continuous Delivery may sequence multiple deployment "rings" for progressive exposure (also known as "controlling the blast radius"). Progressive exposure groups users who get to try new releases to monitor their experience in "rings." The first deployment ring 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

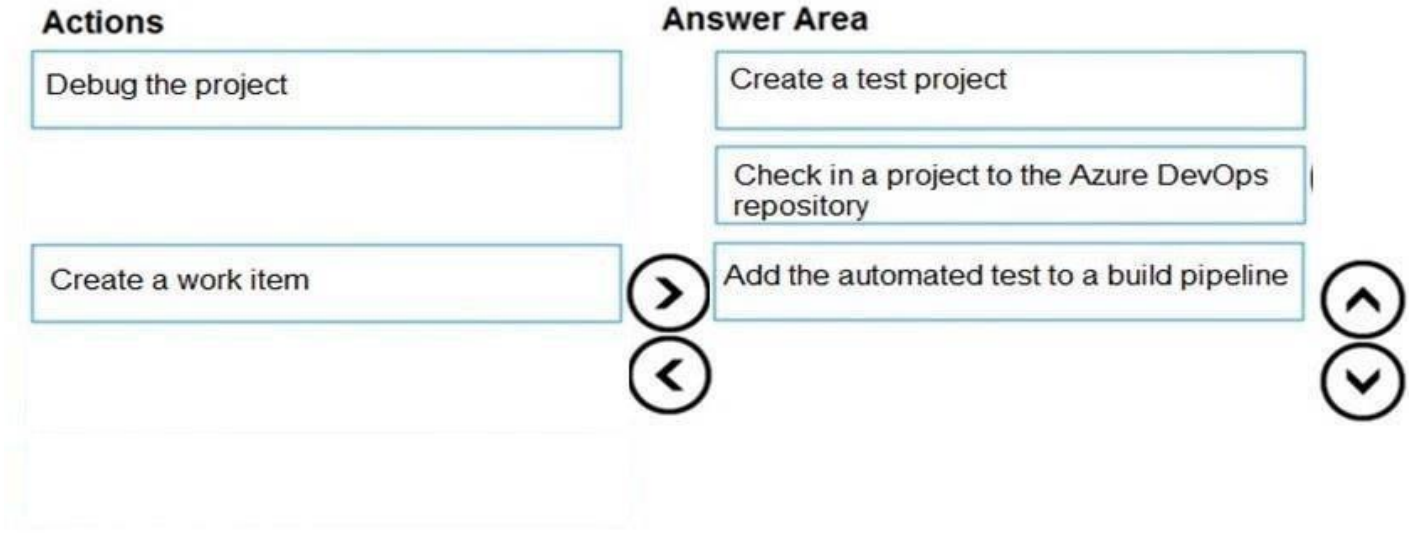
https://medium.com/@denniszielke/continuous-kubernetes-blue-green-deployments-on-azureusing-nginx-appgateway-or-trafficmanager-4490bce29cb

Q239. 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.



A. Debug the project
B. Create a test project[1]
C. Create a work item
D. Check in a project to the Azure DevOps repository[2]
E. Add the automated test to a build pipeline[3]

Answer: BDE



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

Q240. Drag and Drop question

Your company has two virtual machines that run Linux in a third-party public cloud.

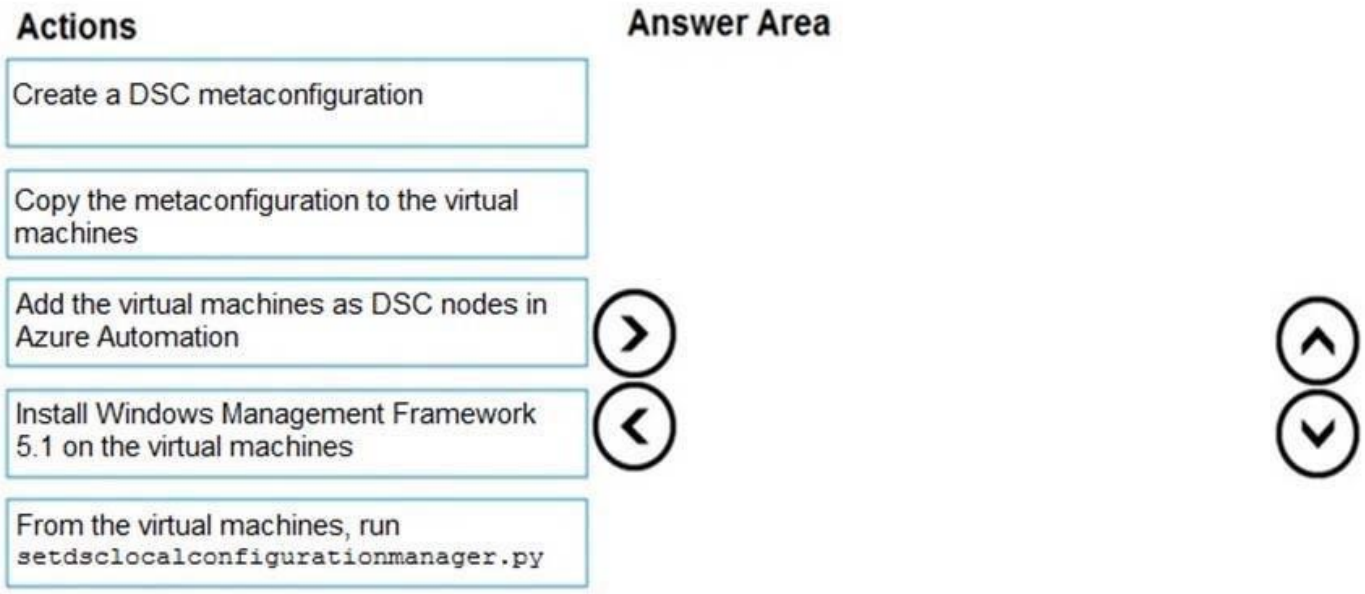
You plan to use the company's Azure Automation State Configuration implementation to manage the two virtual machines and detect configuration drift.

You need to onboard the Linux virtual machines.

You install PowerShell Desired State Configuration (DSC) on the virtual machines, and then run register.py

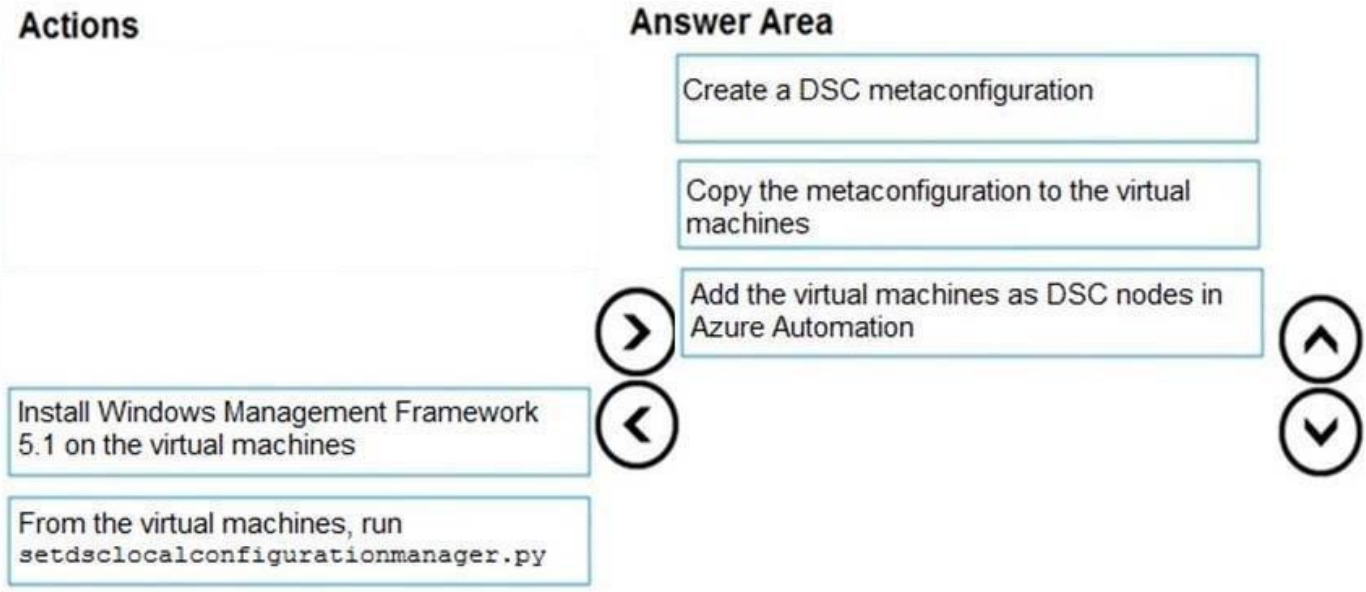
Which three actions should you perform next in sequence?

To answer, move the actions from the list of actions to the answer area and arrange them in the correct order.



A. Create a DSC metaconfiguration[1]
B. Copy the metaconfiguration to the virtual machines[2]
C. Add the virtual machines as DSC nodes in Azure Automation[3]
D. Install Windows Management Framework 5.1 on the virtual machines
E. From the virtual machines, run *setdsclocalconfigurationmanager.py*

Answer: ABC



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.

Q241. 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: CDE