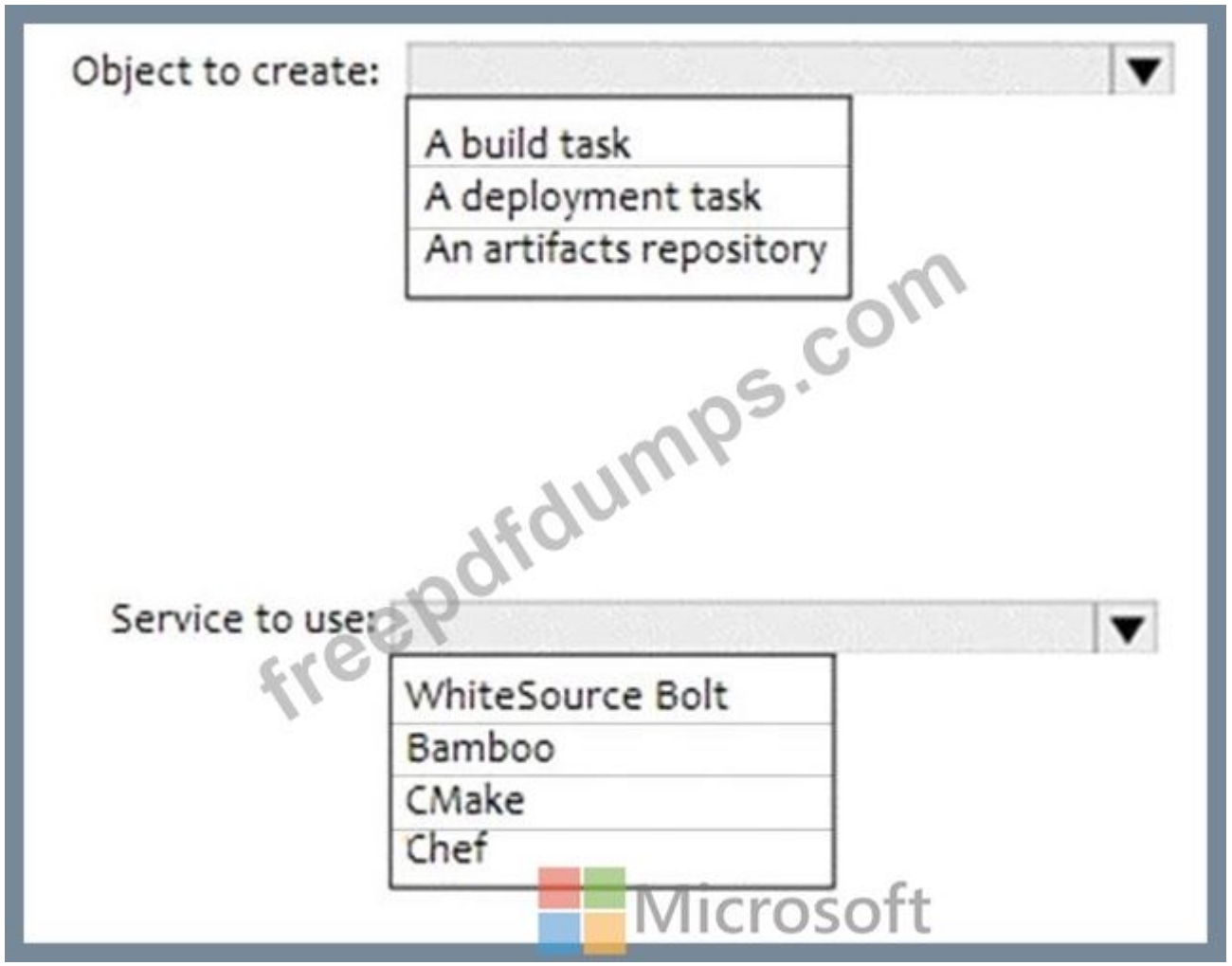
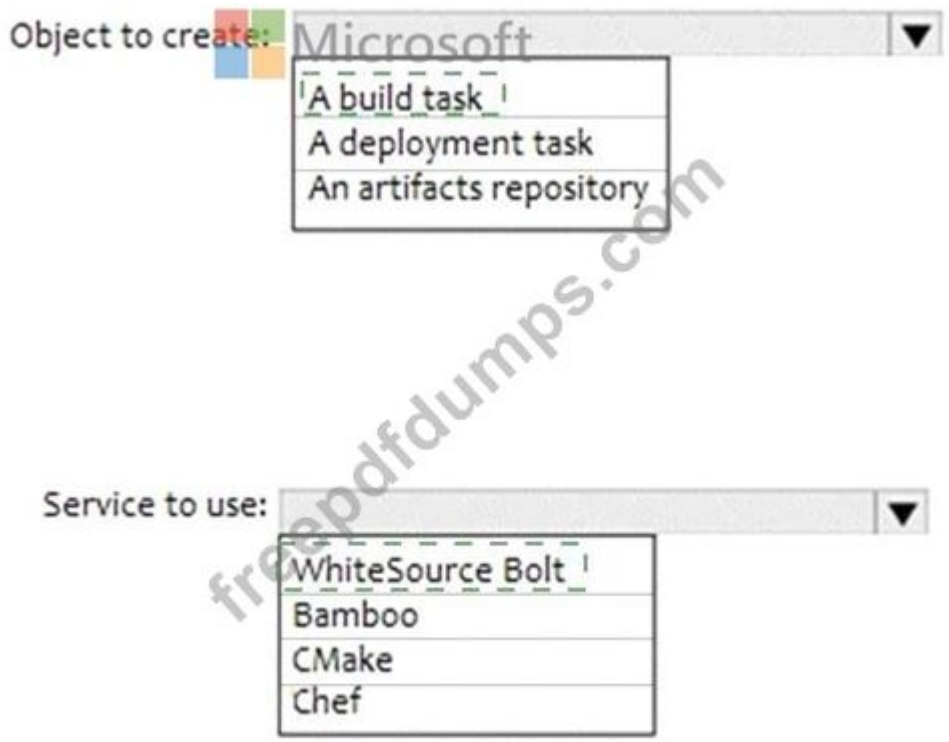
Microsoft.AZ-400.v2021-10-13.q297

Exam Code:	AZ-400
Exam Name:	Designing and Implementing Microsoft DevOps Solutions
Certification Provider:	Microsoft
Free Question Number:	297
Version:	v2021-10-13
# of views:	6818
# of Questions views:	2970
https://www.freepdfdumps.com/Microsoft.AZ-400.v2021-10-13.q297.html	

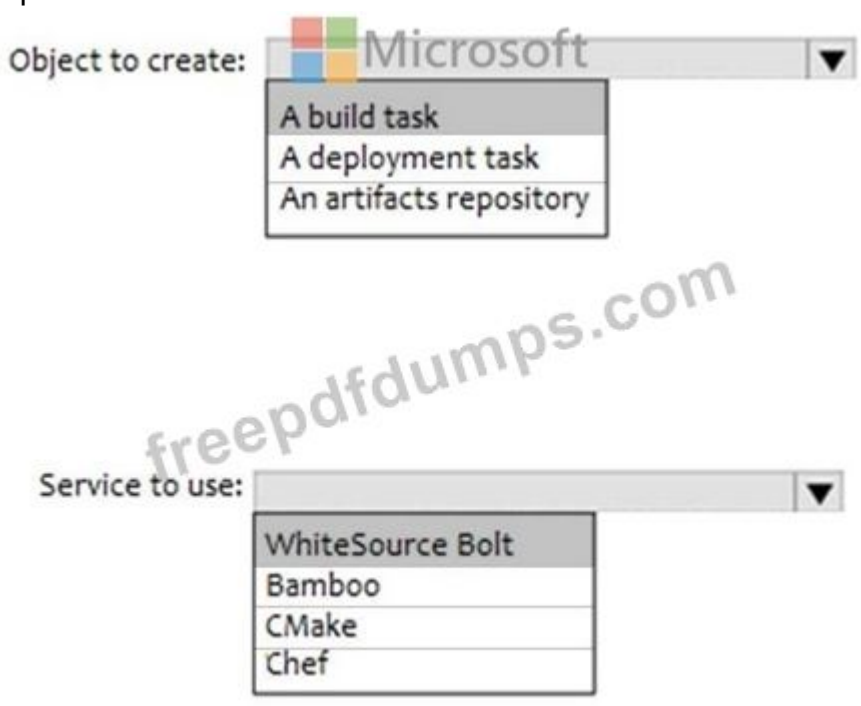
NEW QUESTION: 1
You have an Azure DevOps project that contains a build pipeline. The build pipeline uses approximately 50 open source libraries.
You need to ensure that the project can be scanned for known security vulnerabilities in the open source libraries.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation



Box 1: A Build task

Trigger a build

You have a Java code provisioned by the Azure DevOps demo generator. You will use WhiteSource Bolt extension to check the vulnerable components present in this code.

* Go to Builds section under Pipelines tab, select the build definition WhiteSourceBolt and click on Queue to trigger a build.
* To view the build in progress status, click on ellipsis and select View build results.

Box 2: WhiteSource Bolt

WhiteSource is the leader in continuous open source software security and compliance management.

WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated denitive database of open source repositories.
References:
https://www.azuredevopslabs.com/labs/vstsextend/whitesource/

NEW QUESTION: 2
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 (LEAVE A REPLY)
Explanation
With enterprise level of SonarQube you can use OWASP that runs the security scans for known vulnerabilities.
https://www.sonarqube.org/features/security/
https://www.sonarqube.org/features/security/owasp/?gclid=Cj0KCQiAzZL-BRDnARIsAPCJs70Teq0-efI2Hd_h

NEW QUESTION: 3
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: (SHOW ANSWER)
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.
Reference: https://docs.microsoft.com/en-us/azure/devops/artifacts/feeds/feed-permissions?view=vsts&tabs=new-nav

NEW QUESTION: 4
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an approval process that contains a condition. The condition requires that releases be approved by a team leader before they are deployed.
You have a policy stating that approvals must occur within eight hours.
You discover that deployment fail if the approvals take longer than two hours.
You need to ensure that the deployments only fail if the approvals take longer than eight hours.
Solution: From Pre-deployment conditions, you modify the Time between re-evaluation of gates option.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates

NEW QUESTION: 5
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"]
```

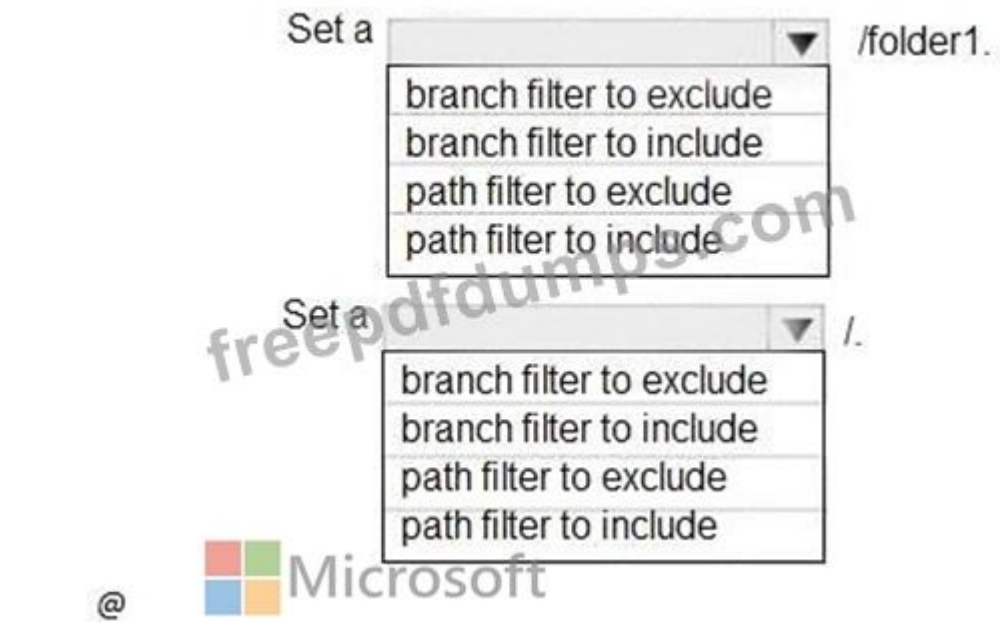
You need to ensure that the image is as small as possible when the image is built.
Which line should you modify in the file?
A. 4
B. 3
C. 7
D. 1
Answer: A (LEAVE A REPLY)

NEW QUESTION: 6
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.
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)

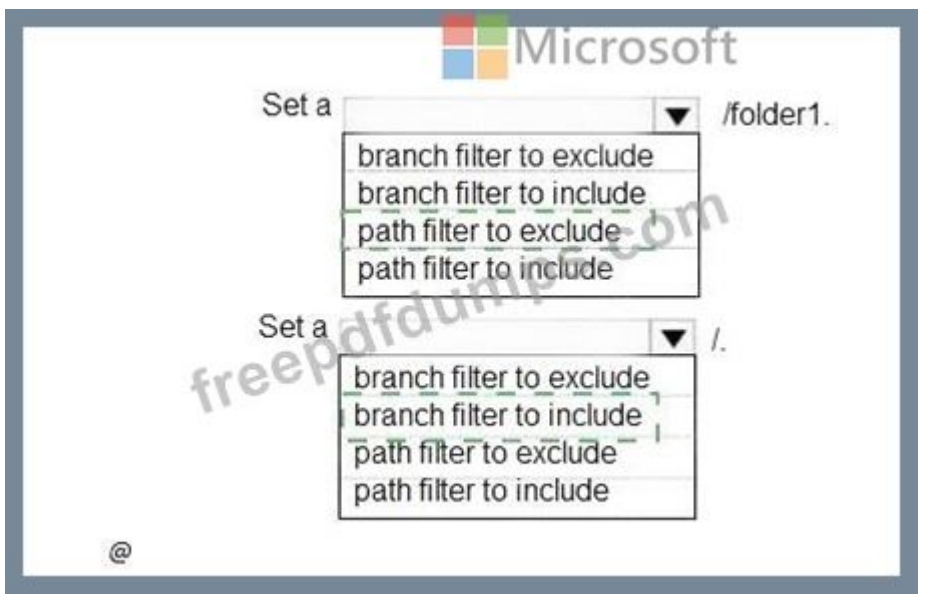
E. the Windows Server 2019 container images hosted in the Azure Container Registry
Ubuntu supported versions: 12.04 LTS, 14.04 LTS, 15.x, 16.04 LTS, 18.04 LTS
Answer: B,C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/deploy-vulnerability-assessment-vm

NEW QUESTION: 7
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: B,C,E (LEAVE A REPLY)
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

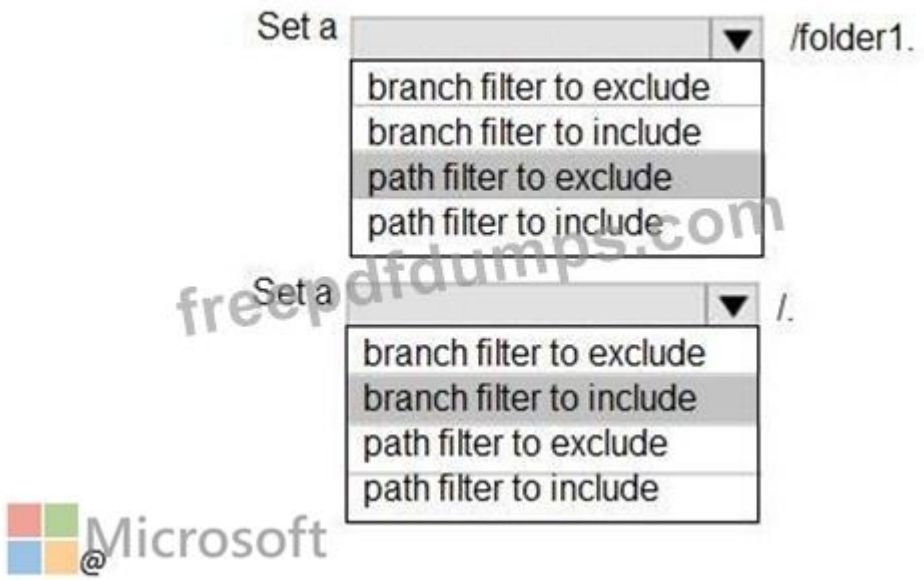
NEW QUESTION: 8
How should you configure the filters for the Project5 trigger? To answer, select the appropriate option in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation



Scenario:

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

NEW QUESTION: 9

You have a project Azure DevOps.

You plan to create a build pipeline that will deploy resources by using Azure Resource Manager templates.

The templates will reference secretes stored in Azure Key Vault.

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

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

NOTE: Each correct selection is worth one point.

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

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

```
  "properties":{
     "mode" : "Incremental",
```

- "deployment"
- "template"
- "templateLink"

```
:{
contentVersion" : "1.0.0.0",
          "uri" : "[uri(parameters('_artifactsLocation'),
          concat('./nested/sqlserver.json',
          parameters('_artifactsLocationSasToken')))]"
      },
      "parameters":{
        "secret":{
          "reference":{
            "keyVault":{
               "id": "[resourceId(parameters('vaultSubscription'),
               parameters('vaultResourceGroupName'),
               'Microsoft.KeyVault/vaults',
               parameters('vaultName'))]"
            },
            "secretName": "[parameters('secretName')]"
             }
            }
          }
        }
      }
    ],
```


Answer:

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

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

```
  "properties":{
     "mode" : "Incremental",
```

:{

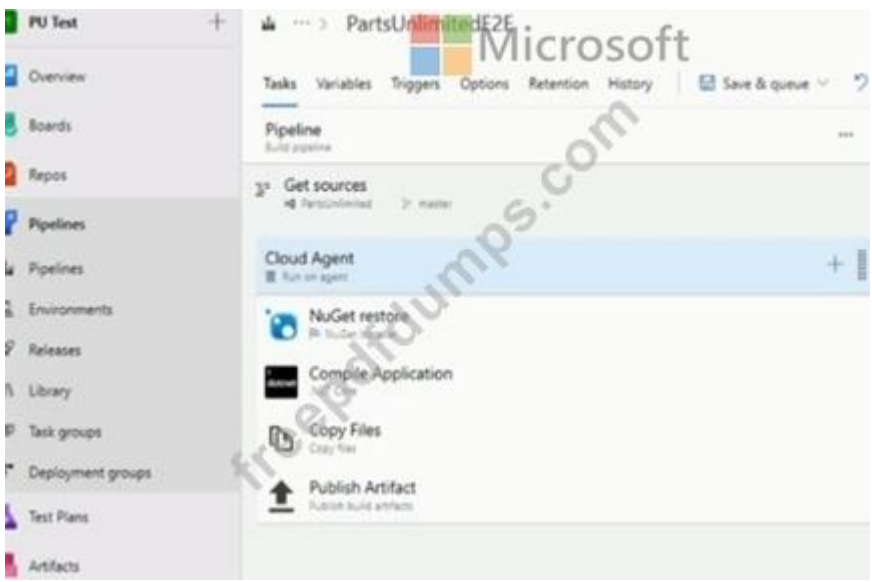
- "deployment"
- "template"
- "templateLink"

```
contentVersion" : "1.0.0.0",
          "uri" : "[uri(parameters('_artifactsLocation'),
          concat('./nested/sqlserver.json',
          parameters('_artifactsLocationSasToken')))]"
      },
      "parameters":{
          "secret":{
             "reference":{
                "keyVault":{
                     "id": "[resourceId(parameters('vaultSubscription'),
                     parameters('vaultResourceGroupName'),
                     'Microsoft.KeyVault/vaults',
                     parameters('vaultName'))]"
                },
                "secretName": "[parameters('secretName')]"
              }
             }
            }
           }
          }
      ],
```

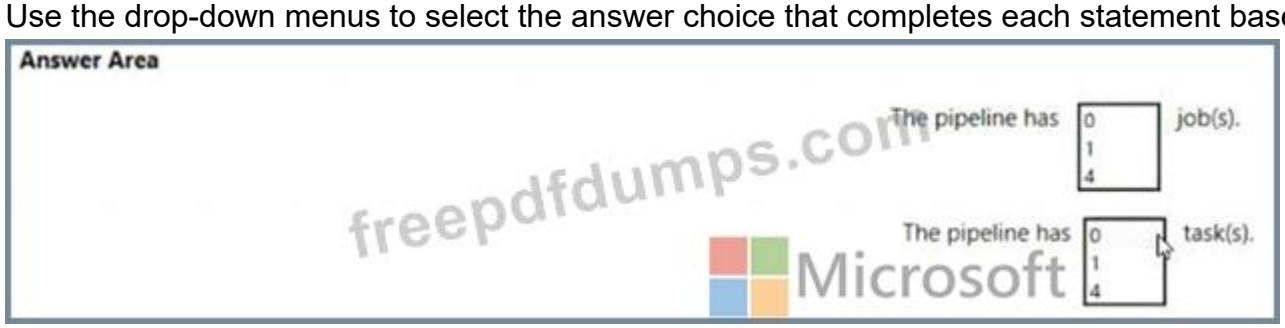

Explanation

NEW QUESTION: 10

You have the Azure DevOps pipeline 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.



Answer:

Explanation

NEW QUESTION: 11

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 (LEAVE A REPLY)
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

NEW QUESTION: 12
You use Azure SQL Database Intelligent Insights and Azure Application Insights foe monitoring.
You need to write ad-hoc Queries against the monitoring data.
Which Query language should you use?
A. PL/pgSQL
B. Transact-SQL
C. Azure Log Analytics
D. PL/SQL
Answer: (SHOW ANSWER)
Data analysis in Azure SQL Analytics is based on Log Analytics language for your custom querying and reporting.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-sql

NEW QUESTION: 13
You ate building an ASP.NET Core application.
You plan to create an application utilization baseline by capturing telemetry data.
You need to add code to the application to capture the telemetry data. The solution must minimize the costs of storing the telemetry data.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A)
Add the `<MaxTelemetryItemsPerSecond>5</MaxTelemetryItemsPerSecond>` parameter to the ApplicationInsights.config file.
B)
From the code of the application, disable adaptive sampling.
C)
From the code of the application, enable adaptive sampling.
D)
Add the `<InitialSamplingPercentage>90</InitialSamplingPercentage>` parameter to the ApplicationInsights.config file.
E)
From the code of the application, add Azure Application Insights telemetry.
A. Option E
B. Option B
C. Option C

D. Option A
E. Option D
Answer: (SHOW ANSWER)

NEW QUESTION: 14
You need to create deployment files for an Azure Kubernetes Service (AKS) cluster. The deployments must meet the provisioning storage requirements shown in the following table.

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

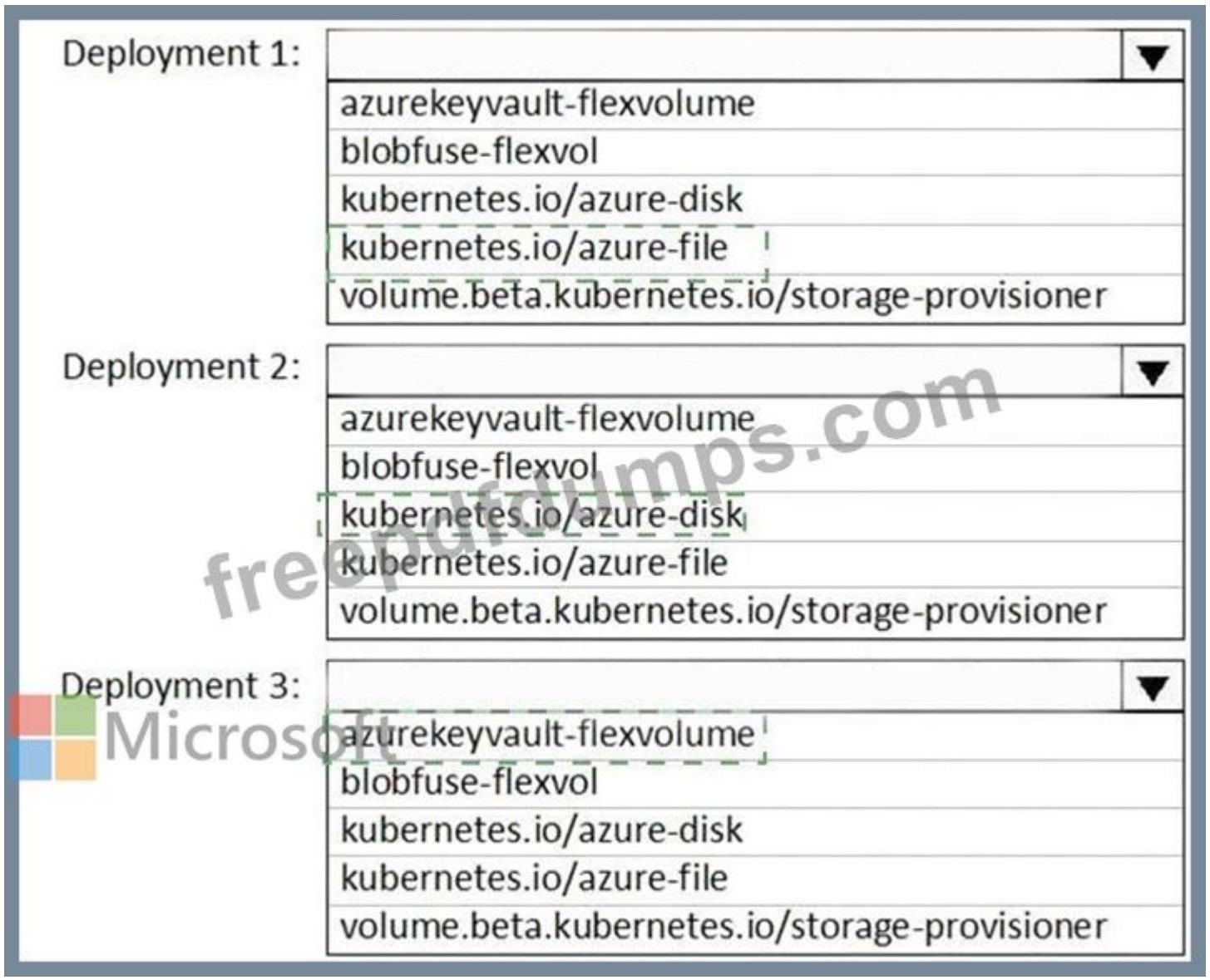
Which resource type should you use for each deployment? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Deployment 1:
- azurekeyvault-flexvolume
- blobfuse-flexvol
- kubernetes.io/azure-disk
- kubernetes.io/azure-file
- volume.beta.kubernetes.io/storage-provisioner

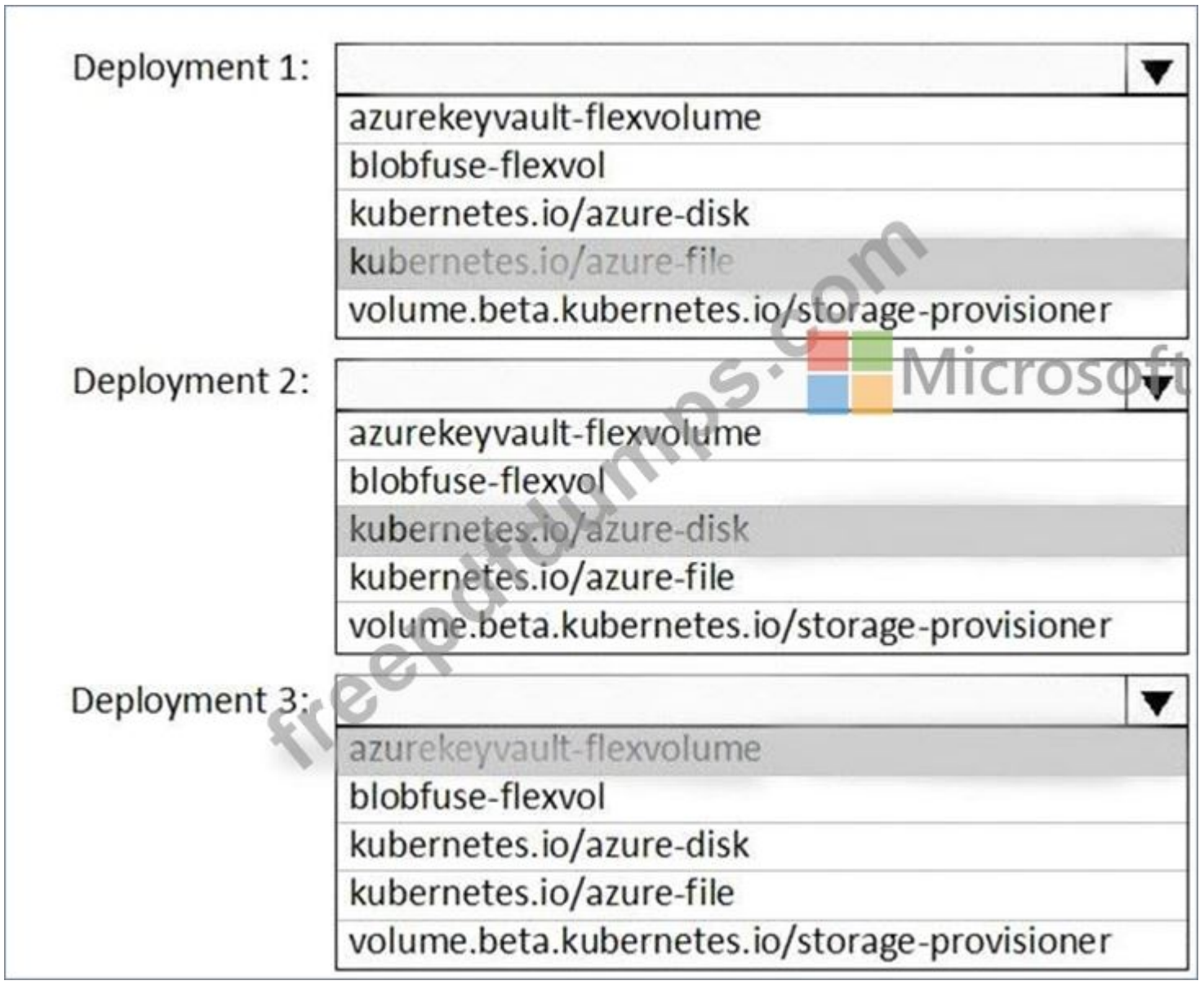
Deployment 2:
- azurekeyvault-flexvolume
- blobfuse-flexvol
- kubernetes.io/azure-disk
- kubernetes.io/azure-file
- volume.beta.kubernetes.io/storage-provisioner

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

Answer:



Explanation



Deployment 1: Kubernetes.io/azure-file

You can use Azure Files to connect using the Server Message Block (SMB) protocol.

Deployment 2: Kubernetes.io/azure-disk

Deployment 3: azurekeyvault-flexvolume

azurekeyvault-flexvolume: Key Vault FlexVolume: Seamlessly integrate your key management systems with Kubernetes.

Secrets, keys, and certificates in a key management system become a volume accessible to pods. Once the volume is mounted, its data is available directly in the container filesystem for your application.

NEW QUESTION: 15

You are developing a multi-tier application. The application will use Azure App Service web apps as the front end and an Azure SQL database as the back end. The application will use Azure functions to write some data to Azure Storage.

You need to send the Azure DevOps team an email message when the front end fails to return a status code of 200.

Which feature should you use?

A. Service Map in Azure Log Analytics

B. Profiler in Azure Application Insights

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

NEW QUESTION: 16
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 changes 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 (LEAVE A REPLY)
Explanation/Reference:
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

NEW QUESTION: 17
You need to ensure that Microsoft Visual Studio 2017 can remotely attach to an Azure Function named fa-11566895.
To complete this task, sign in to the Microsoft Azure portal.
A. Enable Remote Debugging
Before we start a debugging session to our Azure Function app we need to enable the functionality.
* Navigate in the Azure portal to your function app fa-11566895
* Go to the "Application settings"
* Under "Debugging" set Remote Debugging to On and set Remote Visual Studio version to 2017.
B. Enable Remote Debugging

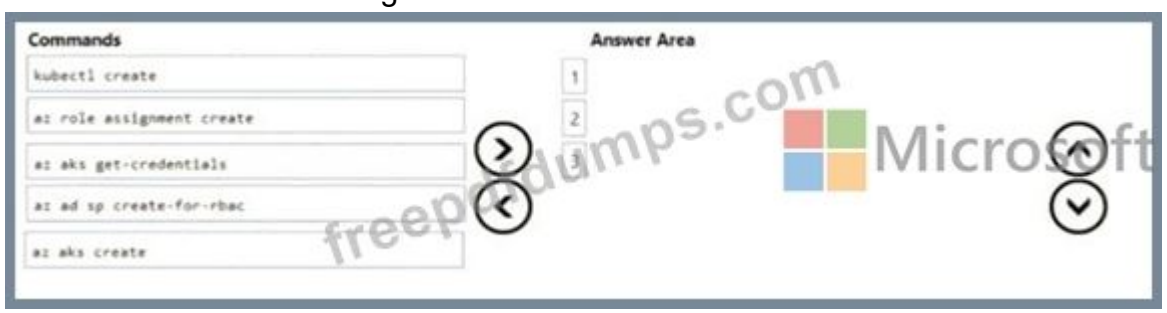
Before we start a debugging session to our Azure Function app we need to enable the functionality.
* Navigate in the Azure portal to your function app fa-11566895
* Go to the "Application settings"
* Under "Debugging" set Remote Debugging to On and set Remote Visual Studio version to 2017.

Answer: (SHOW ANSWER)

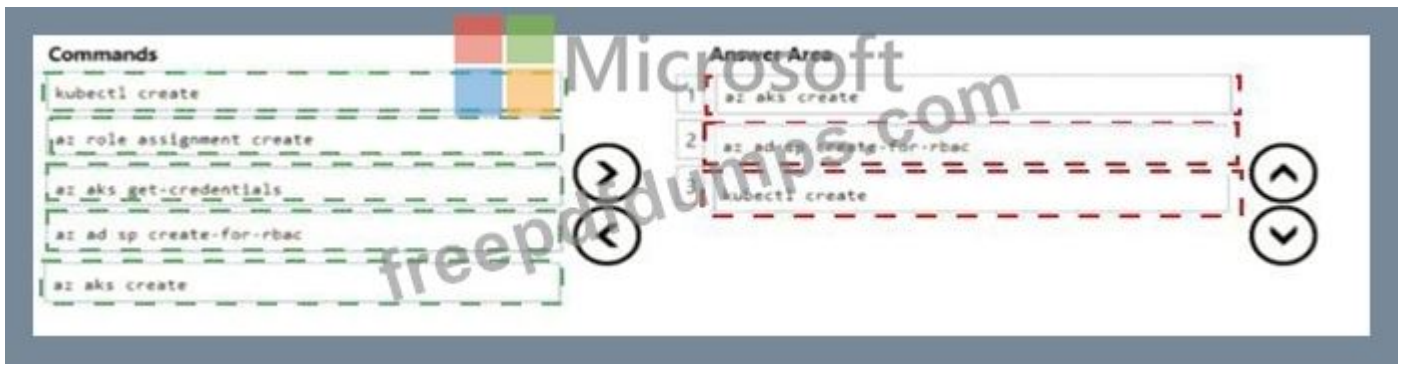
Reference:
https://www.locktar.nl/uncategorized/azure-remote-debugging-manually-in-visual-studio-2017/

NEW QUESTION: 18

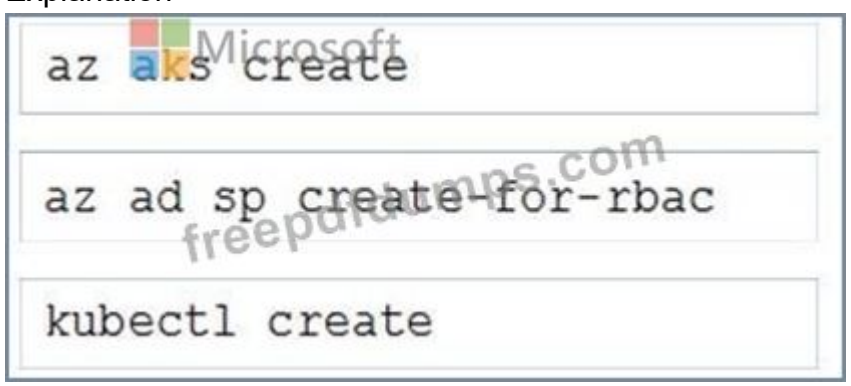
You plan to use Azure Kubernetes Service (AKS) to host containers deployed from images hosted in a Docker Trusted Registry.
You need to recommend a solution for provisioning and connecting to AKS. The solution must ensure that AKS is RBAC-enaWed and uses a custom service principal.
Which three commands should you recommend be run in sequence? To answer, move the appropriate commands from the list of commands to the answer area and arrange them in the coned order.



Answer:



Explanation



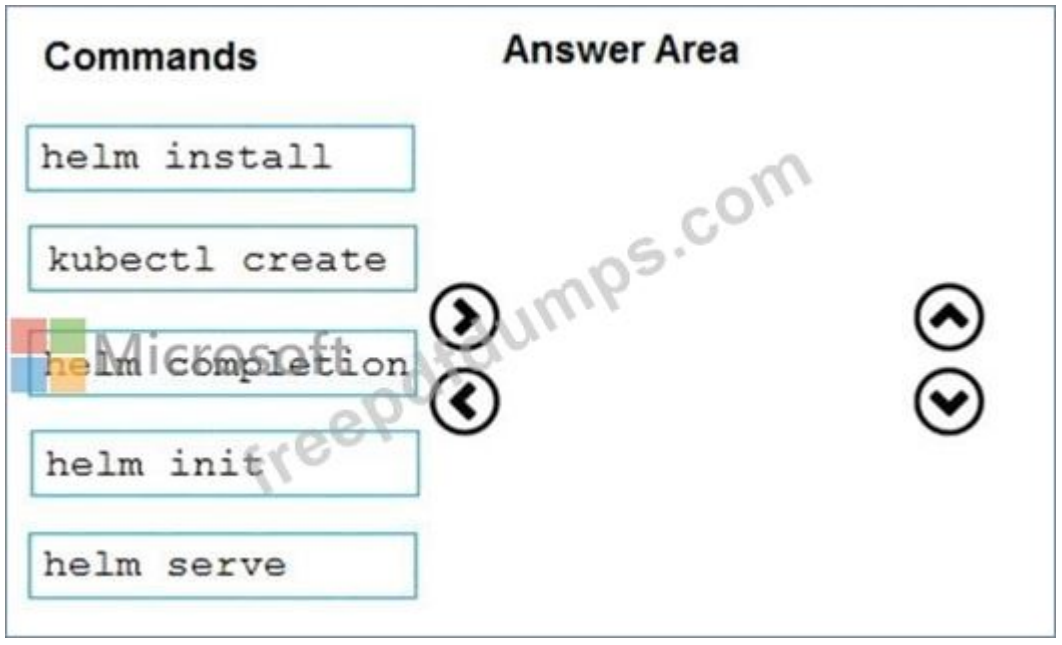
Step 1 : az acr create
An Azure Container Registry (ACR) can also be created using the new Azure CLI.
az acr create

--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/re
--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

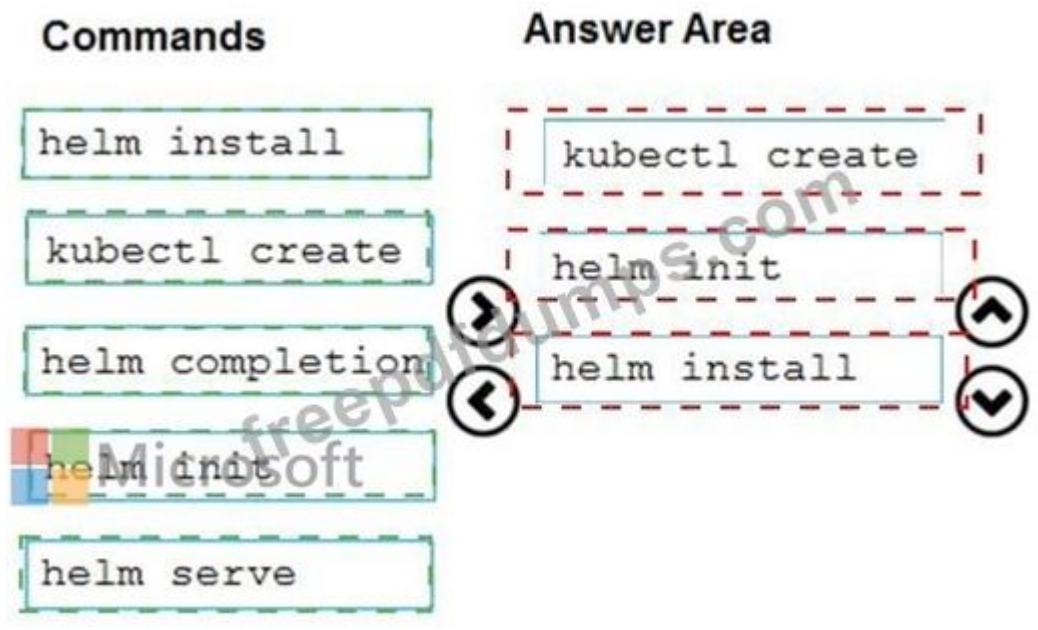
NEW QUESTION: 19
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a project in Azure DevOps for a new web application.
You need to ensure that when code is checked in, a build runs automatically.
Solution: From the Pre-deployment conditions settings of the release pipeline, you select After stage.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Use a Pull request trigger.
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/build/triggers

NEW QUESTION: 20
You provision an Azure Kubernetes Service (AKS) cluster that has RBAC enabled. You have a Helm chart for a client application.
You need to configure Helm and Tiller on the cluster and install the chart.

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



Answer:



Explanation

Step 1: Kubectl create

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

Example: Service account with cluster-admin role
$ kubectl create -f rbac-config.yaml
serviceaccount "tiller" created
clusterrolebinding "tiller" created
$ helm init --service-account tiller
Step 2: helm init
To deploy a basic Tiller into an AKS cluster, use the helm init command.
Step 3: helm install
To install charts with Helm, use the helm install command and specify the name of the chart to install.
References:
https://docs.microsoft.com/en-us/azure/aks/kubernetes-helm
https://docs.helm.sh/using_helm/#tiller-namespaces-and-rbac

NEW QUESTION: 21
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:
* The builds must access an on-premises dependency management system.
* The build outputs must be stored as Server artifacts in Azure DevOps.
* The source code must be stored in a Git repository in Azure DevOps.
Solution: Configure the build pipeline to use a Hosted VS 2019 agent pool. Include the Java Tool Installer task in the build pipeline.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Instead use Octopus Tentacle.
References:
https://explore.emtecinc.com/blog/octopus-for-automated-deployment-in-devops-models

NEW QUESTION: 22
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.

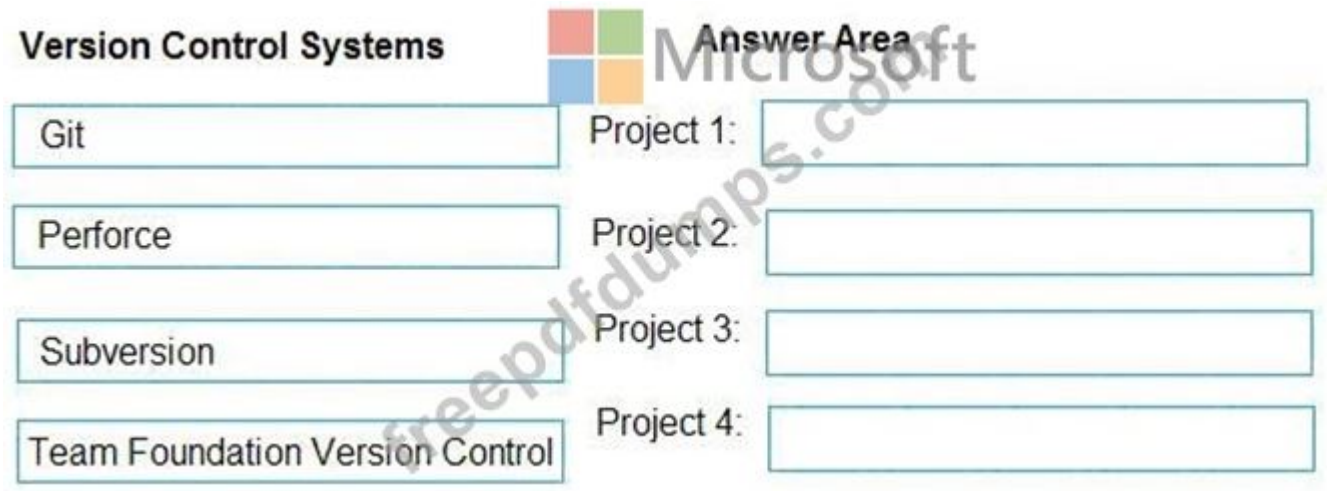
You plan to use Azure Repos for all the projects.

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

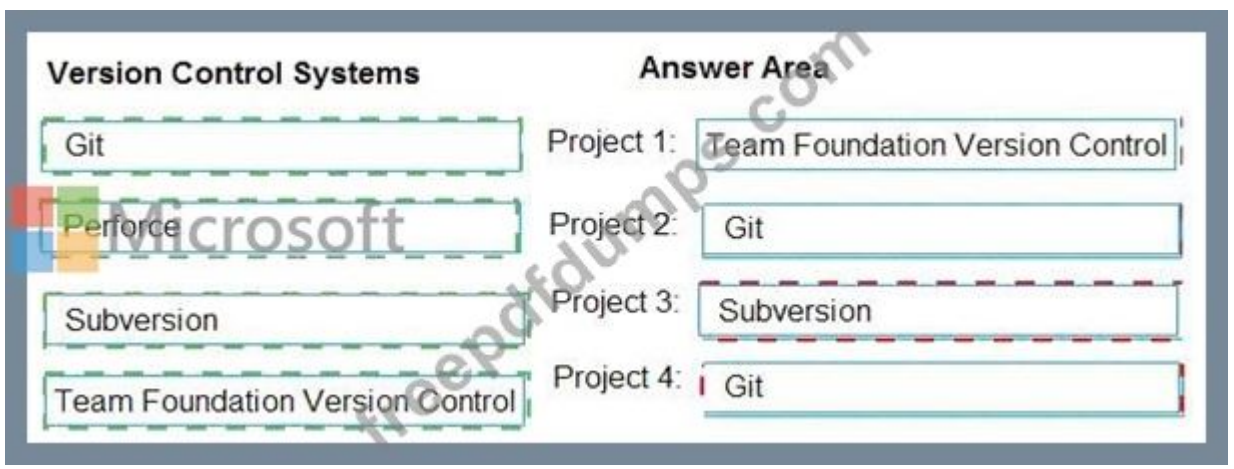
Each version control system may be used once, more than once, or not at all.

You may need to drag the split bar between panes or scroll to view content.

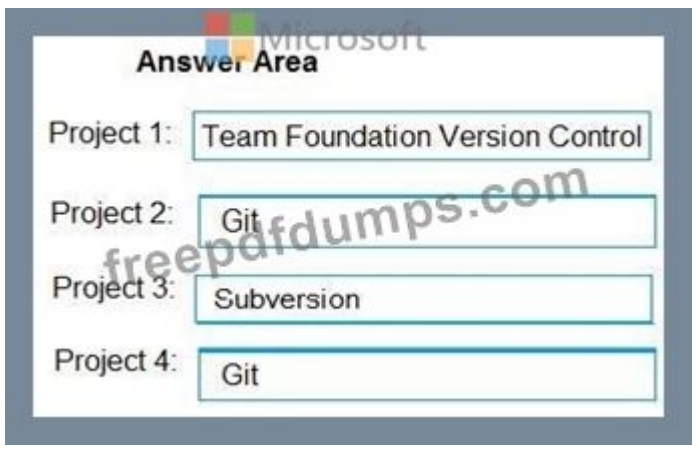
NOTE: Each correct selection is worth one point.



Answer:



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

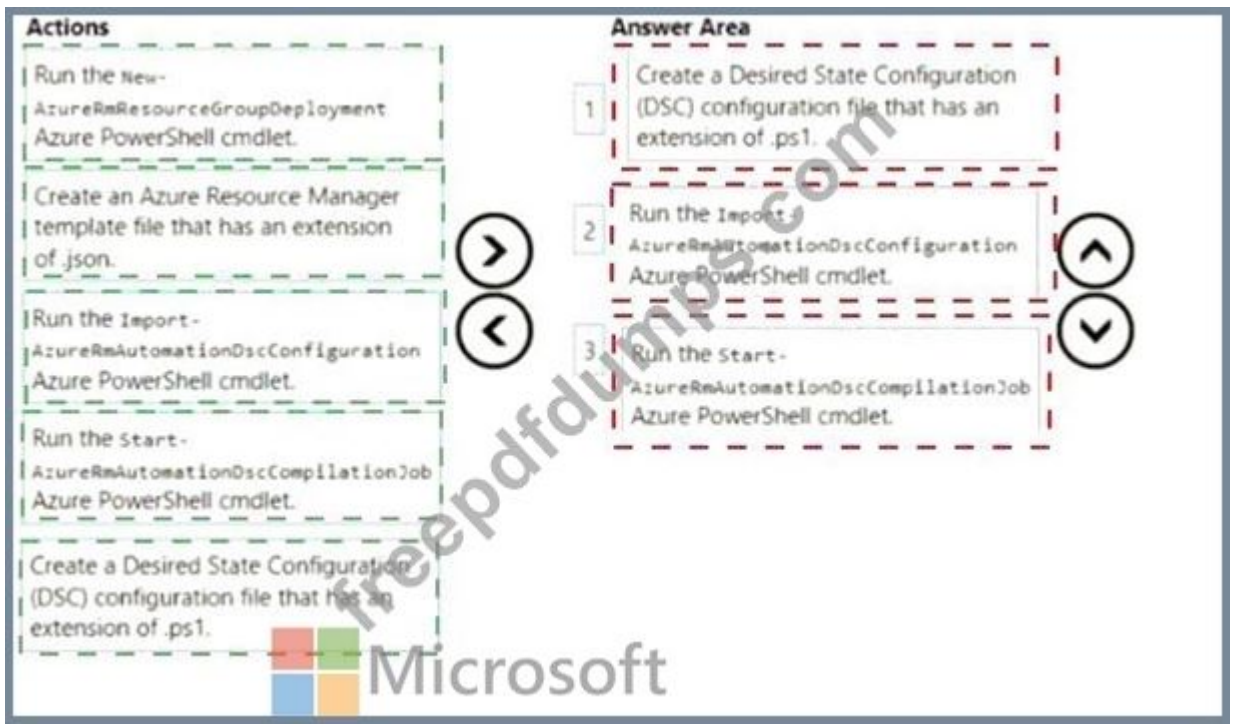
https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/overview

NEW QUESTION: 23

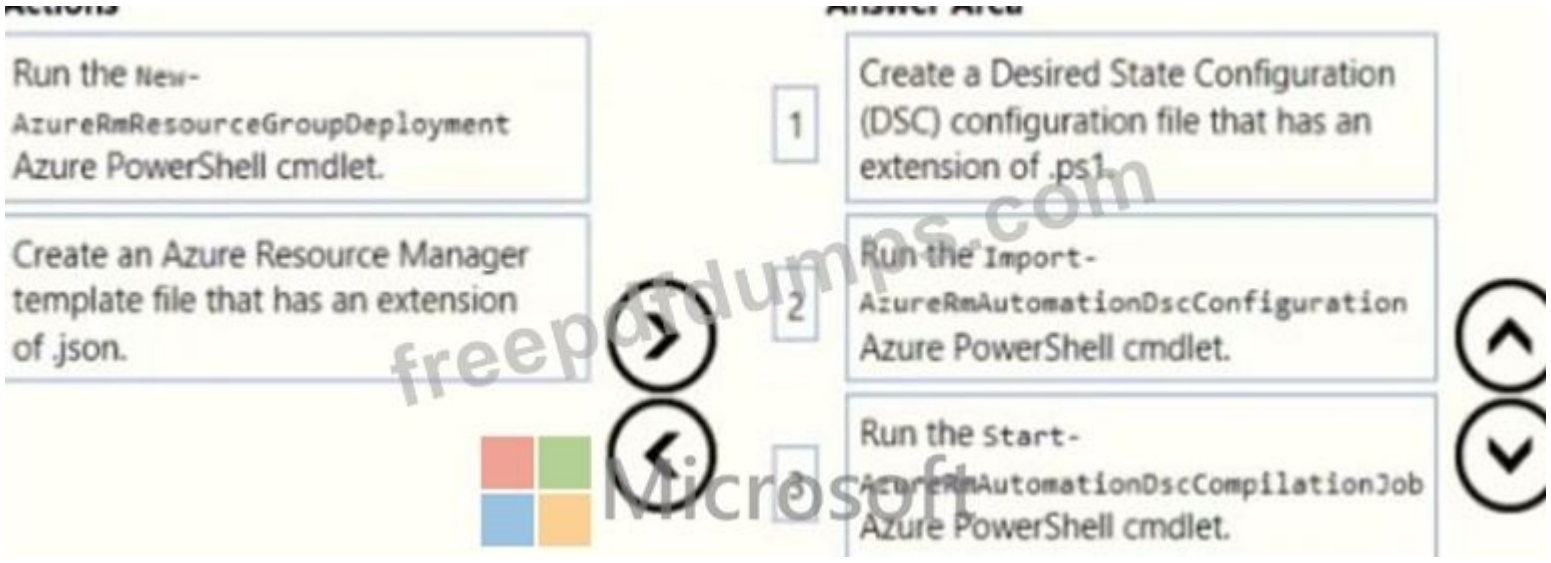
You need to configure Azure Automation for the computers in Pool7.

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

Answer:



Explanation



NEW QUESTION: 24

Your 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:

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.

Reference:

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

NEW QUESTION: 25

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: C (LEAVE A REPLY)

Explanation

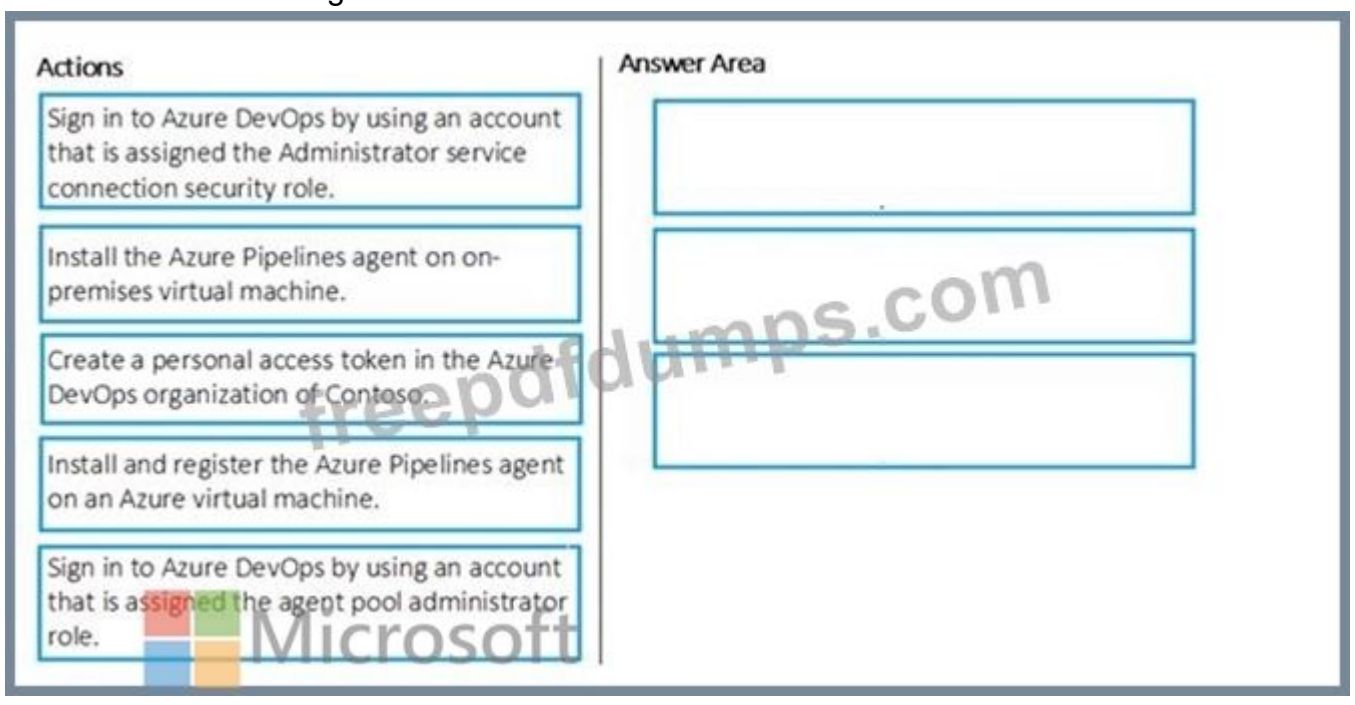
"Build and test with a multi-stage Dockerfile: build and tests execute inside the container using a multi-stage Docker file, as such test results are not published back to the pipeline."

https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-test-results?view=azure-devops&tabs

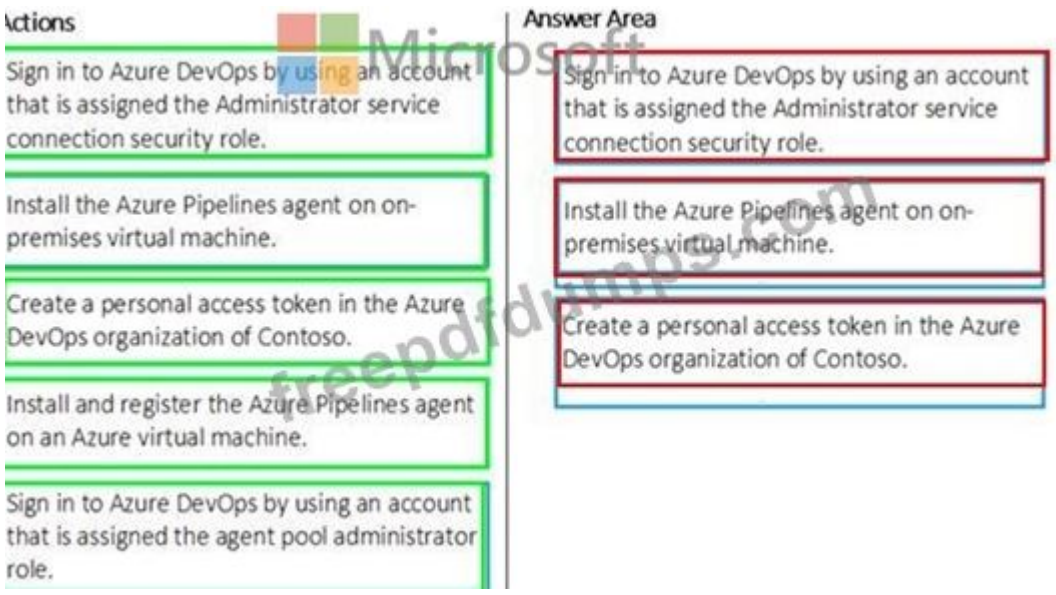
NEW QUESTION: 26

You need to recommend a procedure to implement the build agent for Project1.

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



Answer:



Explanation:

Scenario:

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

Step 1: Sign in to Azure Devops by using an account that is assigned the Administrator service connection security role.

Note: Under Agent Phase, click Deploy Service Fabric Application. Click Docker Settings and then click Configure Docker settings. In Registry Credentials Source, select Azure Resource Manager Service Connection. Then select your Azure subscription.

Step 2: Create a personal access token..

A personal access token or PAT is required so that a machine can join the pool created with the Agent Pools (read, manage) scope.

Step 3: Install and register the Azure Pipelines agent on an Azure virtual machine.

By running a Azure Pipeline agent in the cluster, we make it possible to test any service, regardless of type.

References:

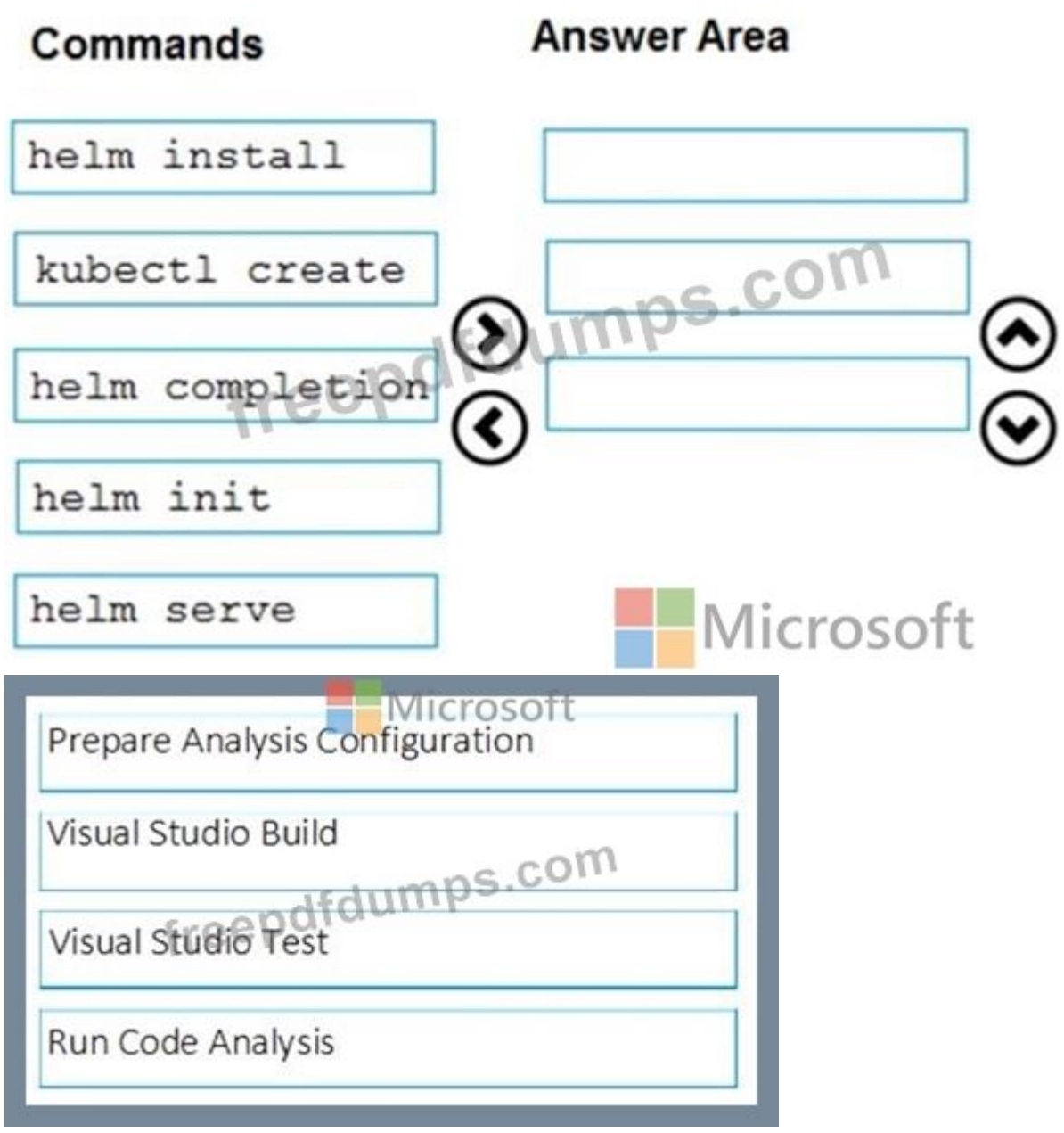
https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-tutorial-deploy-container-app-with-cicd-vsts

NEW QUESTION: 27

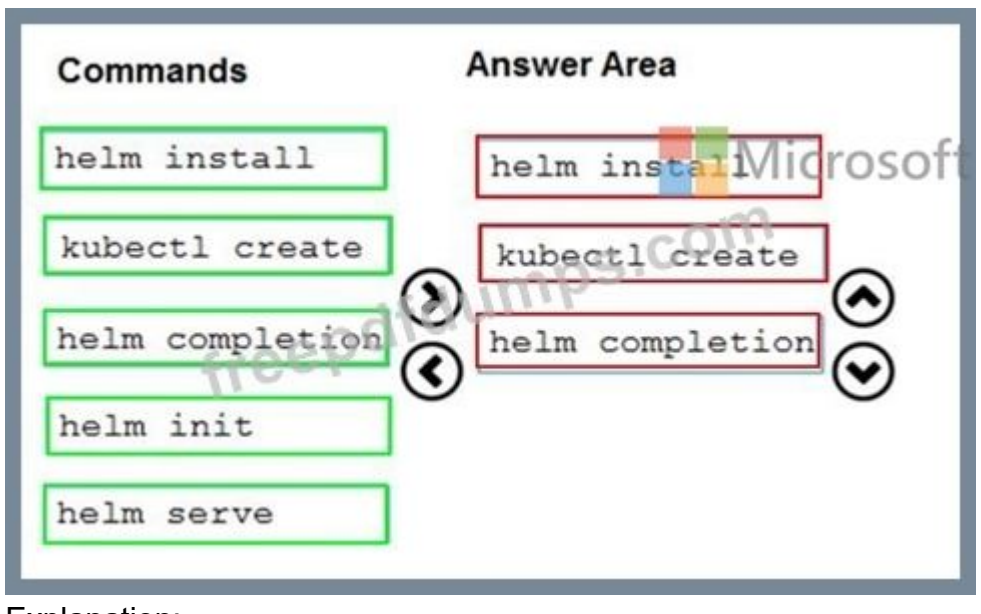
You are developing a full Microsoft .NET Framework solution that includes unit tests.

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.



Answer:



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

NEW QUESTION: 28
You have an Azure DevOps organization named Contoso.
You have 10 Azure virtual machines that run Windows Server 2019. The virtual machines host an application that you build and deploy by using Azure Pipelines. Each virtual machine has the Web Server (IIS) role installed and configured.
You need to ensure that the web server configurations pin the virtual machines is maintained automatically.
The solution must provide centralized management of the configuration settings and minimize management overhead.

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

Answer:

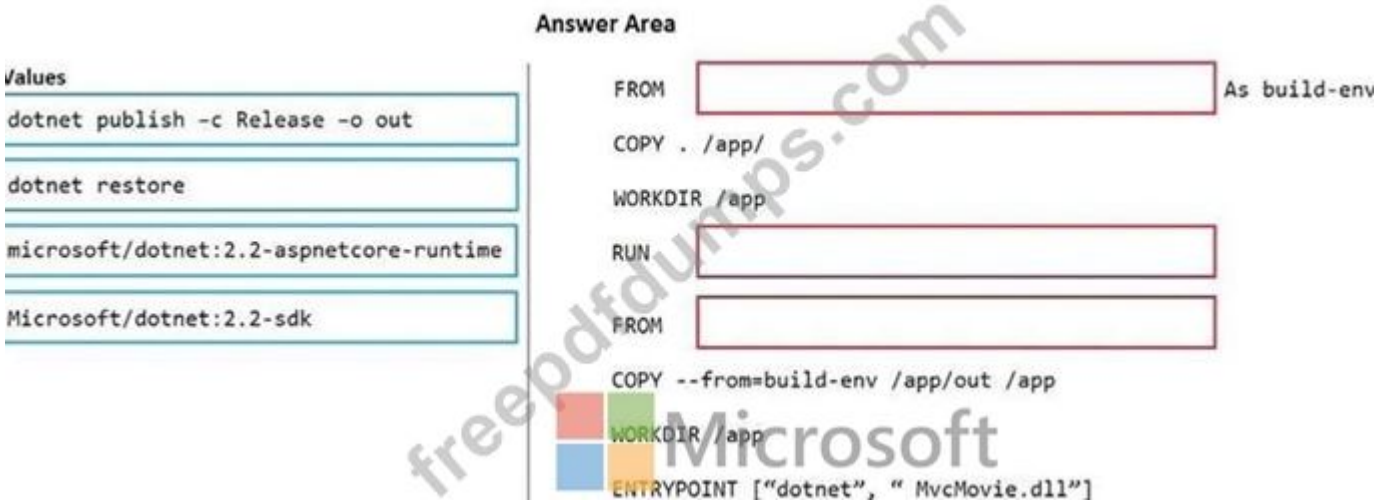
NEW QUESTION: 29

You are creating a container for an ASP.NET Core app.

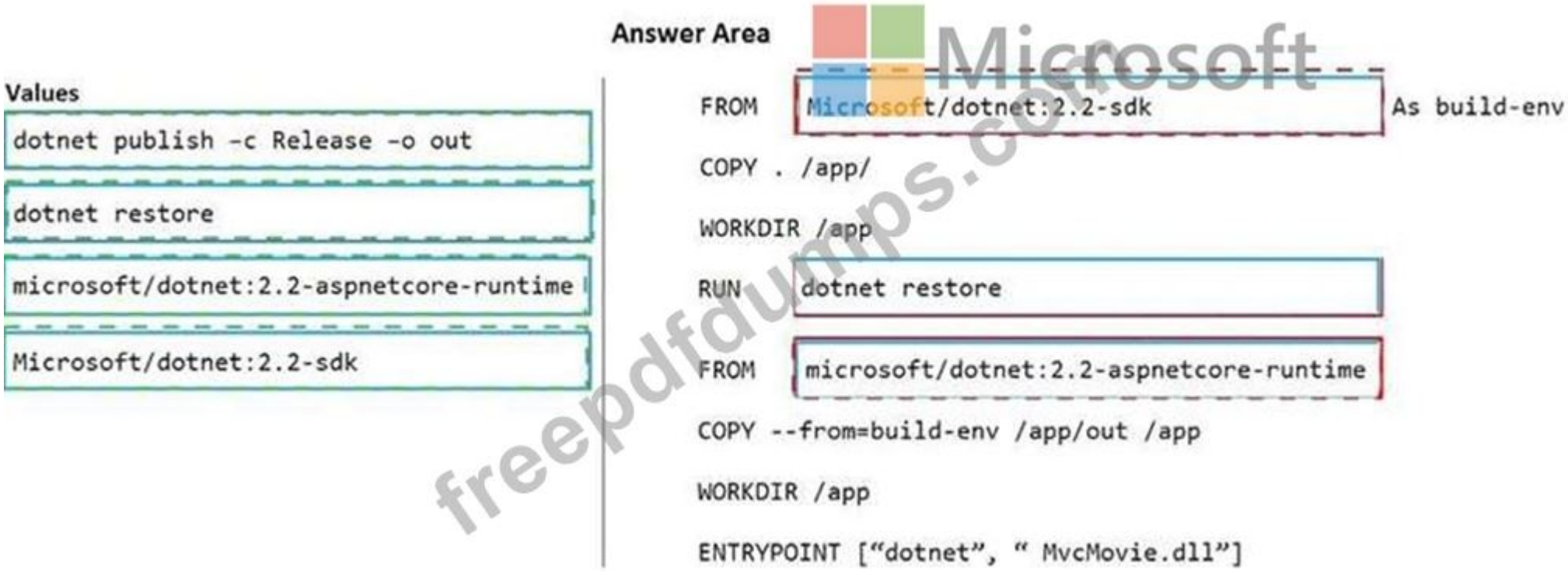
You need to create a Dockerfile file to build the image. The solution must ensure that the size of the image is minimized.

How should you configure the file? To answer, drag the appropriate values to the correct targets. Each value must be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

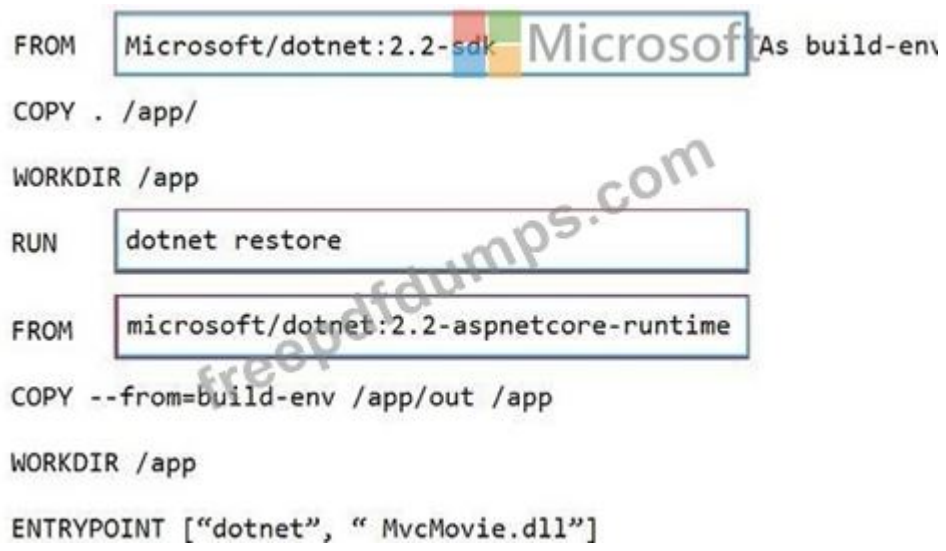
NOTE: Each correct selection is worth one point.



Answer:



Explanation



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

The first group of lines declares from which base image we will use to build our container on top of. If the local system does not have this image already, then docker will automatically try and fetch it. The mcr.microsoft.com/dotnet/core/sdk:2.1 comes packaged with the .NET core 2.1 SDK installed, so it's up to the task of building ASP .NET core projects targeting version 2.1 Box 2: dotnet restore The next instruction changes the working directory in our container to be /app, so all commands following this one execute under this context.

COPY *.csproj ./

RUN dotnet restore

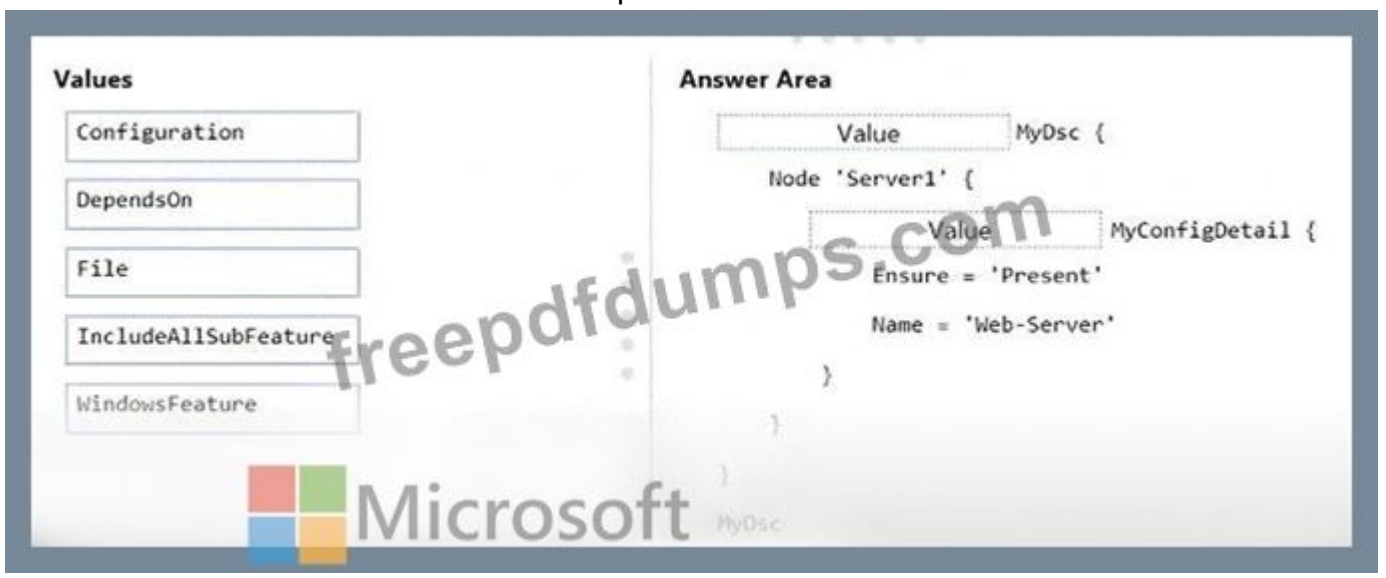
Box 3: microsoft.com/dotnet/2.2-aspnetcore-runtime

When building container images, it's good practice to include only the production payload and its dependencies in the container image. We don't want the .NET core SDK included in our final image because we only need the .NET core runtime, so the dockerfile is written to use a temporary container that is packaged with the SDK called build-env to build the app.

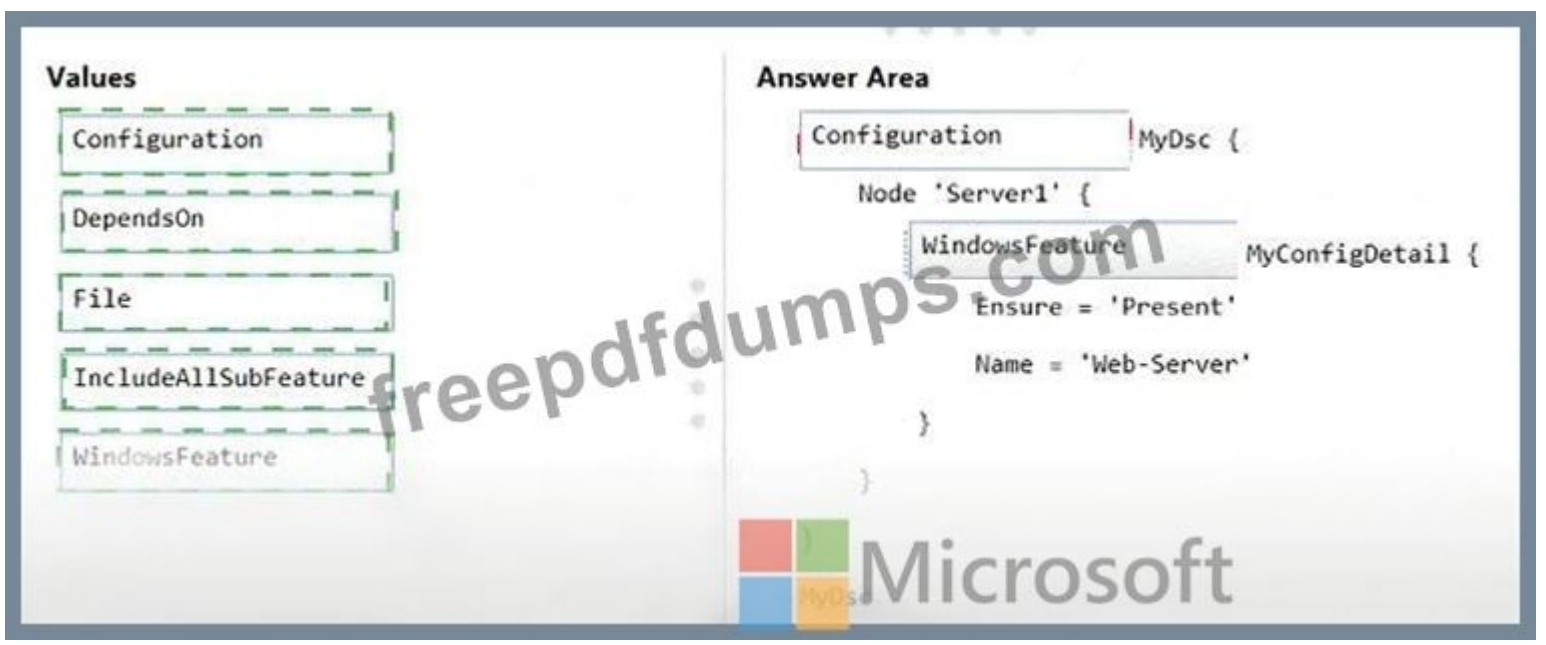
Reference:

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

NEW QUESTION: 30
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 (DSQ 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.



Answer:



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

NEW QUESTION: 31

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

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

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

Two resource groups

Four Azure virtual machines in one resource group

Two Azure SQL databases in other resource group

You need to recommend a solution to deploy the resources.

Solution: Create a single standalone template that will deploy all the resources.

Does this meet the goal?

A. Yes
B. No
Answer: B (LEAVE A REPLY)
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

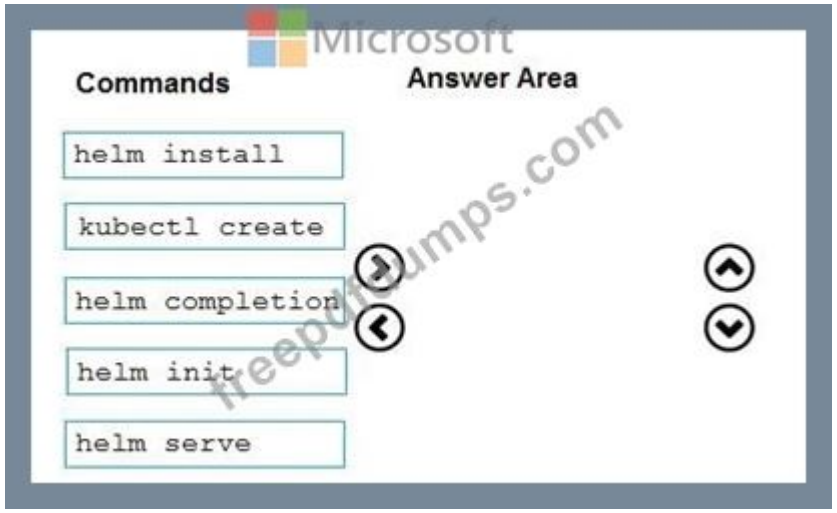
NEW QUESTION: 32
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You plan to update the Azure DevOps strategy of your company.
You need to identify the following issues as they occur during the company's development process:
* Licensing violations
* Prohibited libraries
Solution: You implement automated security testing.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
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/

NEW QUESTION: 33
You need to configure a cloud service to store the secrets required by the mobile applications to call the share.
What should you include in the solution? To answer, select the appropriate options m the answer atea, NOTE:
Each correct selection is worth one point.

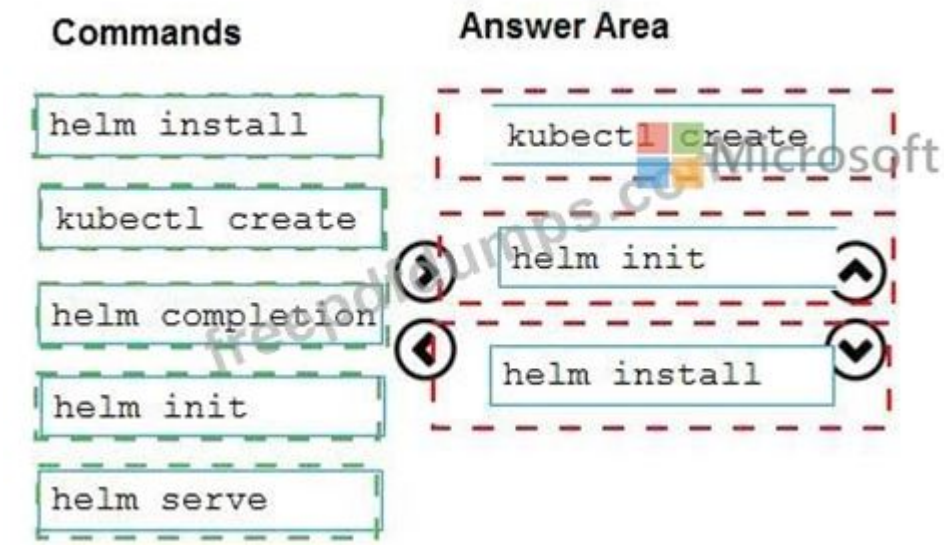
Answer:

NEW QUESTION: 34

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



Answer:



Explanation

Step 1: Kubectl create

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

Example: Service account with cluster-admin role

$ kubectl create -f rbac-config.yaml

serviceaccount "tiller" created

clusterrolebinding "tiller" created

$ helm init --service-account tiller

Step 2: helm init

To deploy a basic Tiller into an AKS cluster, use the helm init command.

Step 3: helm install

To install charts with Helm, use the helm install command and specify the name of the chart to install.

References:

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

https://docs.helm.sh/using_helm/#tiller-namespaces-and-rbac

NEW QUESTION: 35

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

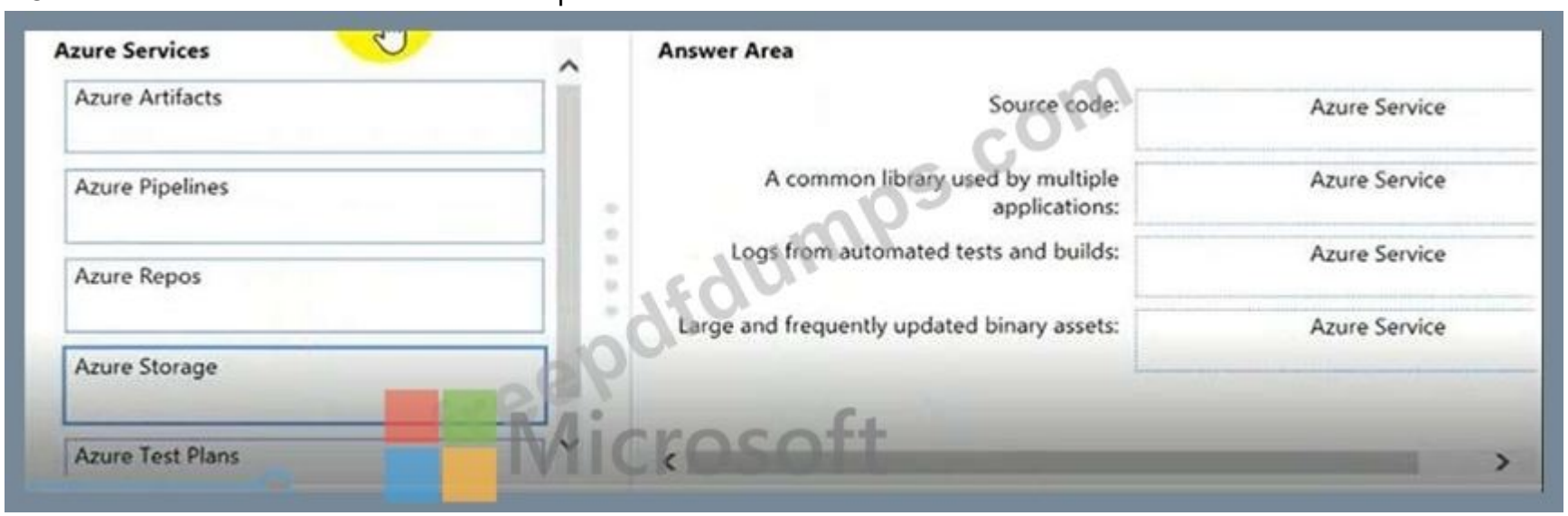
You need to recommend a solution to capture and store telemetry data. The solution must meet the following requirements:

* Support using ad-hoc queries to identify baselines.

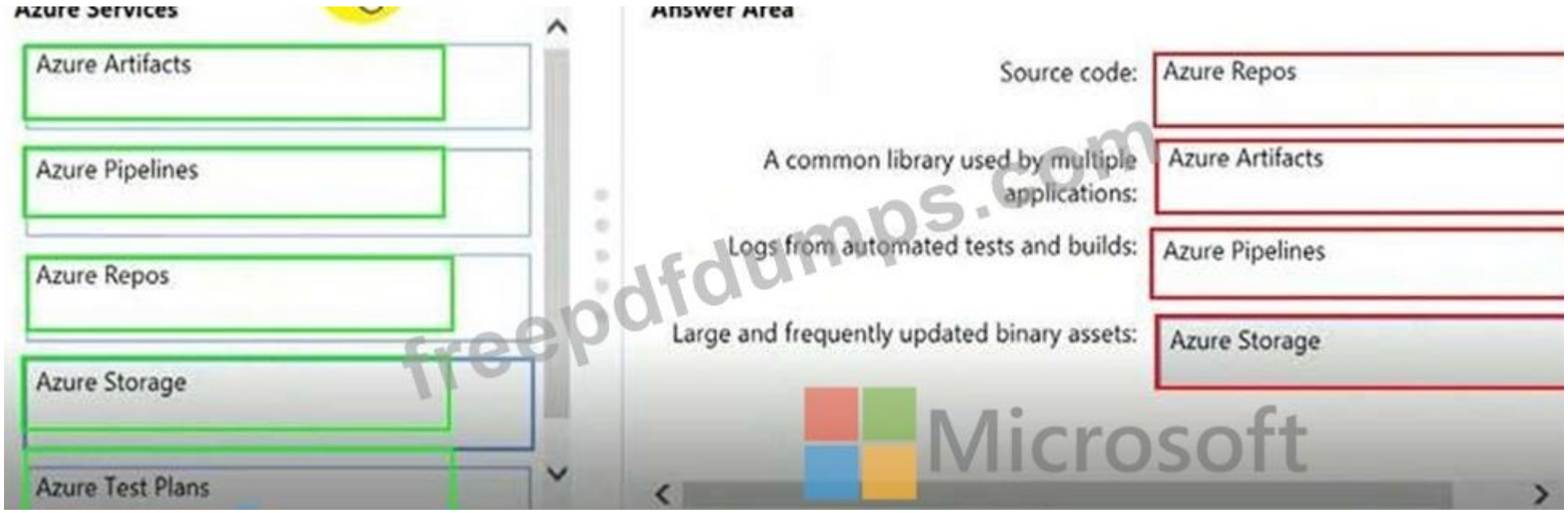
* Trigger alerts when metrics in the baseline are exceeded.

* Store application and database metrics in a central location.
What should you include in the recommendation?
A. Azure Event Hubs
B. Azure SQL Database Intelligent Insights
C. Azure Application Insights
D. Azure Log Analytics
Answer: (SHOW ANSWER)
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.
Incorrect Answers:
B: Intelligent Insights analyzes database performance by comparing the database workload from the last hour with the past seven-day baseline workload. However, we need handle application metrics as well.
References: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-azurepass-posh

NEW QUESTION: 36
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.



Answer:



Explanation:

Box 1: Azure Repos

Box 2: Azure Artifacts

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

Box 3: Azure Pipelines

In the pipeline view you can see all the stages and associated tests. The view provides a summary of the test results Box 4: Azure Storage

Reference:

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

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

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

NEW QUESTION: 37

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

You need to add code coverage testing and publish the outcomes to the pipeline.

What should you use?

A. Bullseye Coverage

B. JUnit

C. JaCoCo

D. NUnit

Answer: C (LEAVE A REPLY)

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:

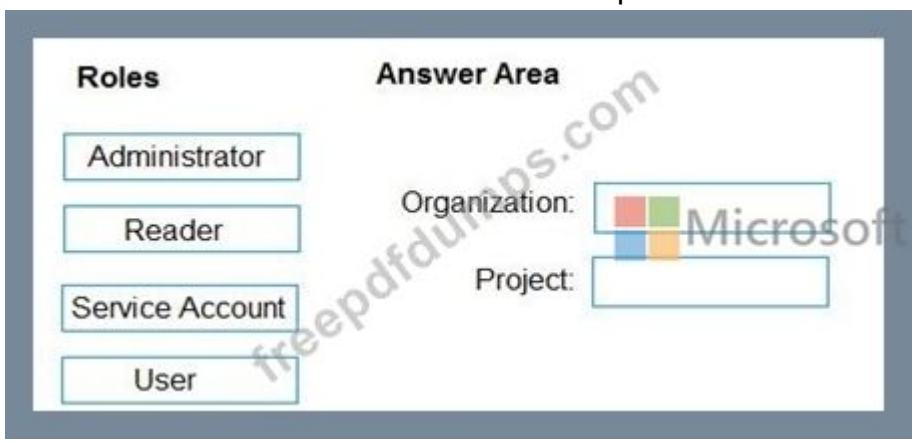
A: Bullseye Coverage is used for C++ code, and not for Java.

Reference:

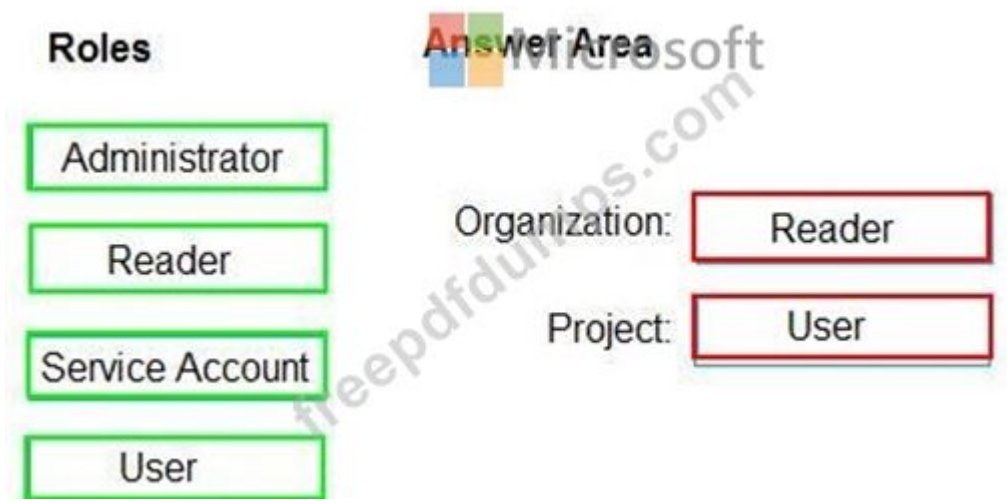
https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-code-coverage-results

NEW QUESTION: 38

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

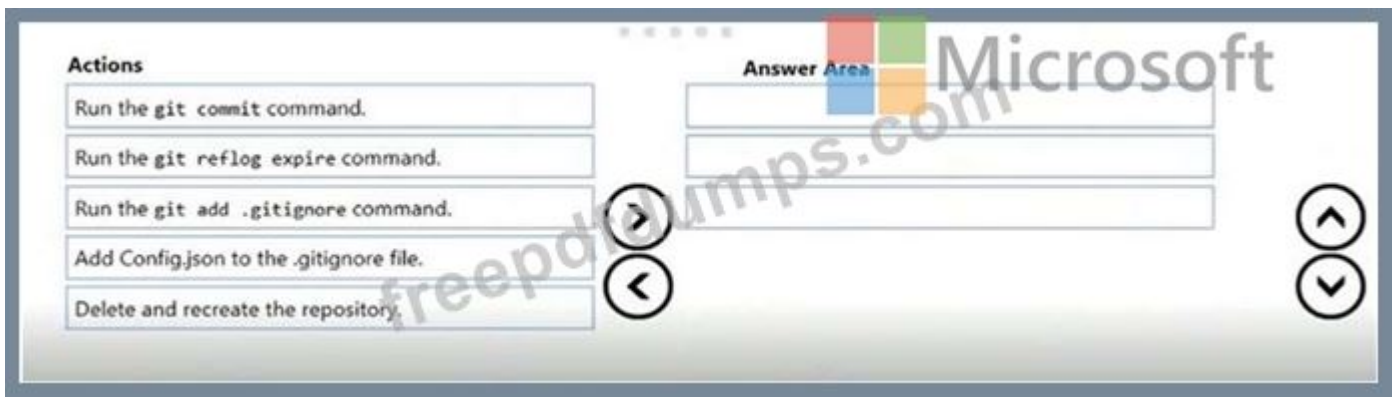


Answer:

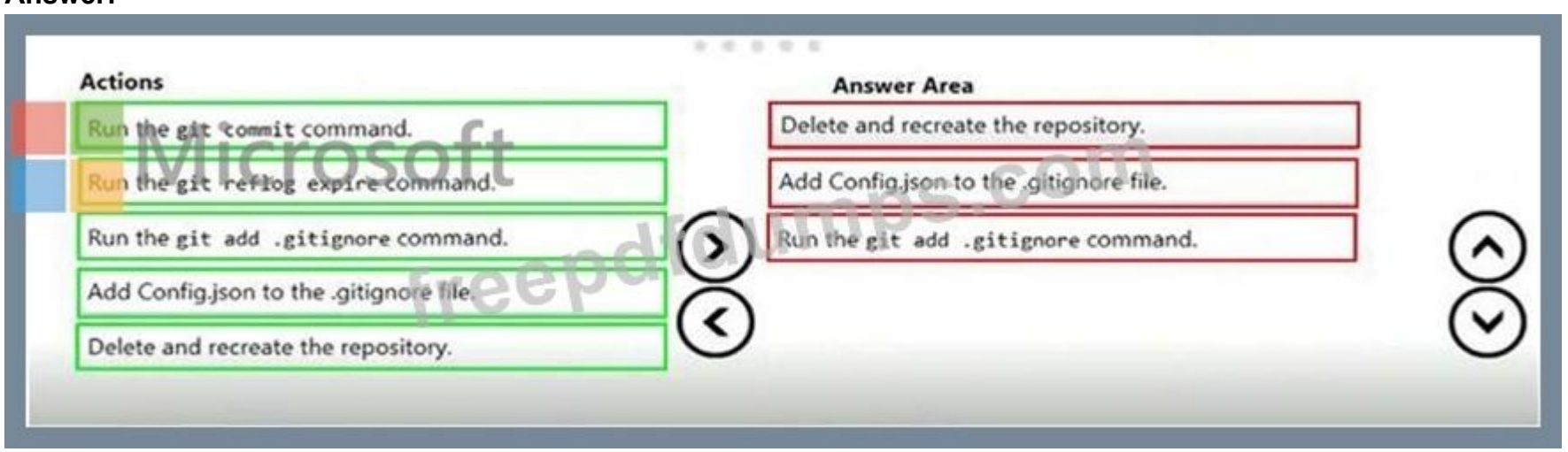


Explanation:
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues

NEW QUESTION: 39
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.



Answer:



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/

NEW QUESTION: 40

You are creating a build pipeline in Azure Pipelines.

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

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

What should you do?

A. Configure the build pipeline to use parallel jobs

B. Configure flaky tests

C. Increase the test pass percentage
D. Add the Requirements quality widget to your dashboard
Answer: D (LEAVE A REPLY)
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

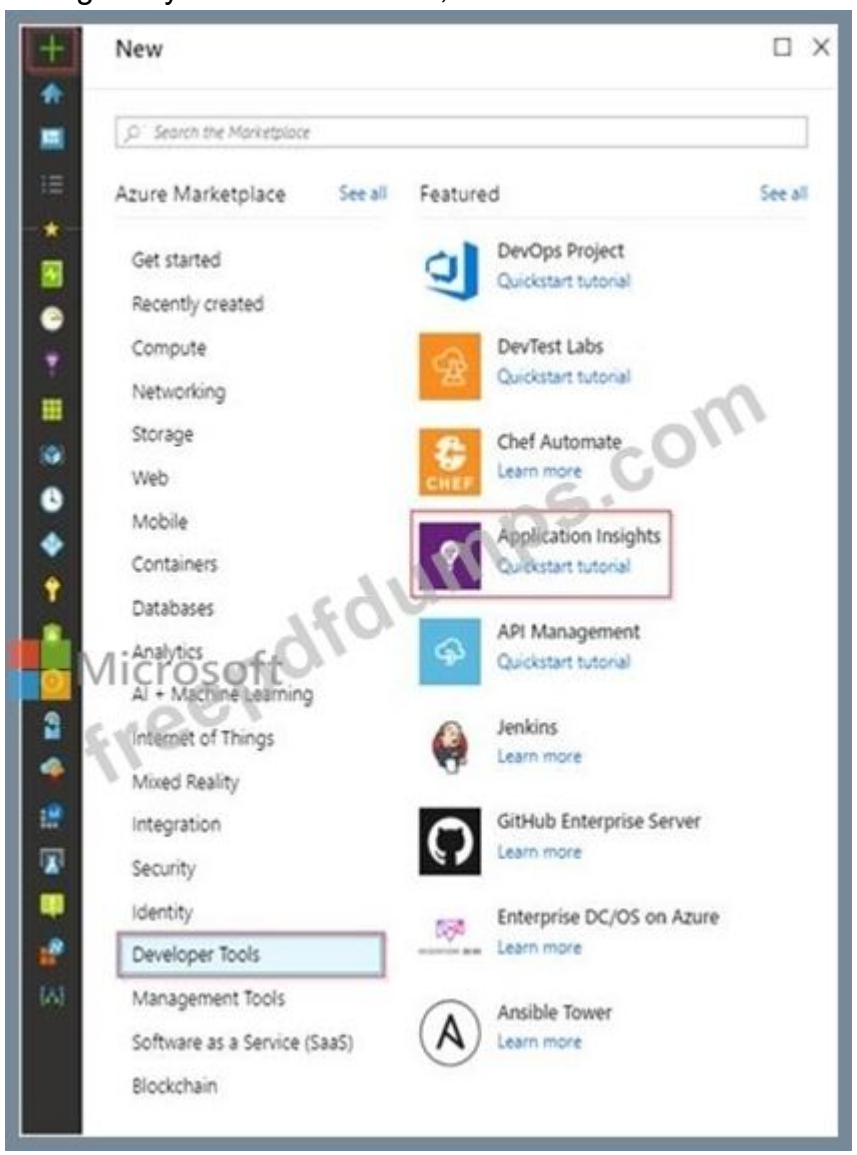
NEW QUESTION: 41
You have an Azure DevOps organization named Contoso and an Azure DevOps project named Project1.
You plan to use Microsoft-hosted agents to build container images that will host full Microsoft .NET Framework apps in a YAML pipeline in Project1.
What are two possible virtual machine images 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: B,C (LEAVE A REPLY)
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

NEW QUESTION: 42
SIMULATION
You need to create an instance of Azure Application Insights named az400-9940427-main and configure the instance to receive telemetry data from an Azure web app named az400-9940427-main.
To complete this task, sign in to the Microsoft Azure portal.

A. Step 1: Create an instance of Azure Application Insights

1. Open Microsoft Azure Portal

2. Log into your Azure account, Select Create a resource > Developer tools > Application Insights.

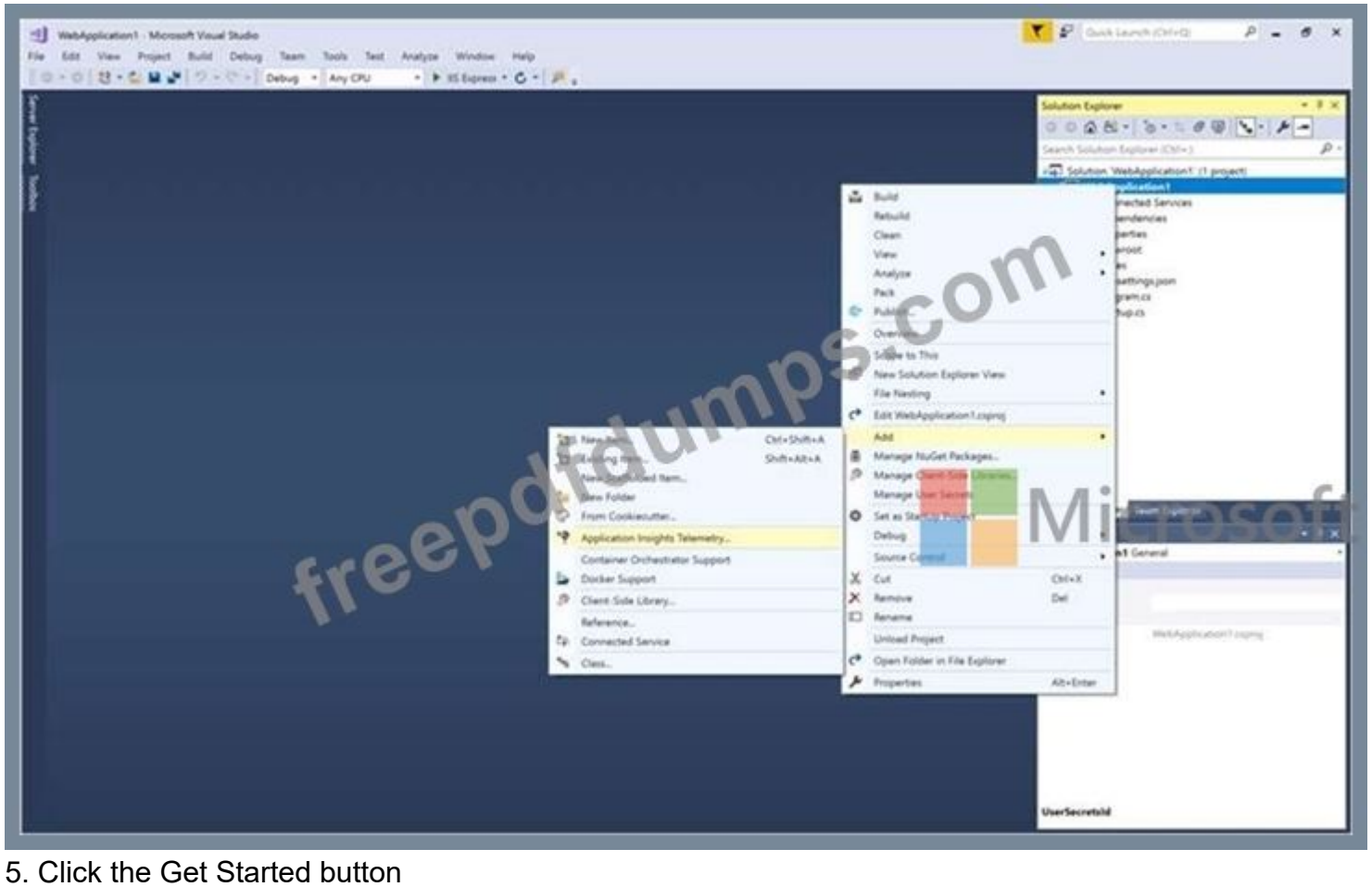


3. Enter the following settings, and then select Review + create.

Name: az400-9940427-main

Step 2: Configure App Insights SDK

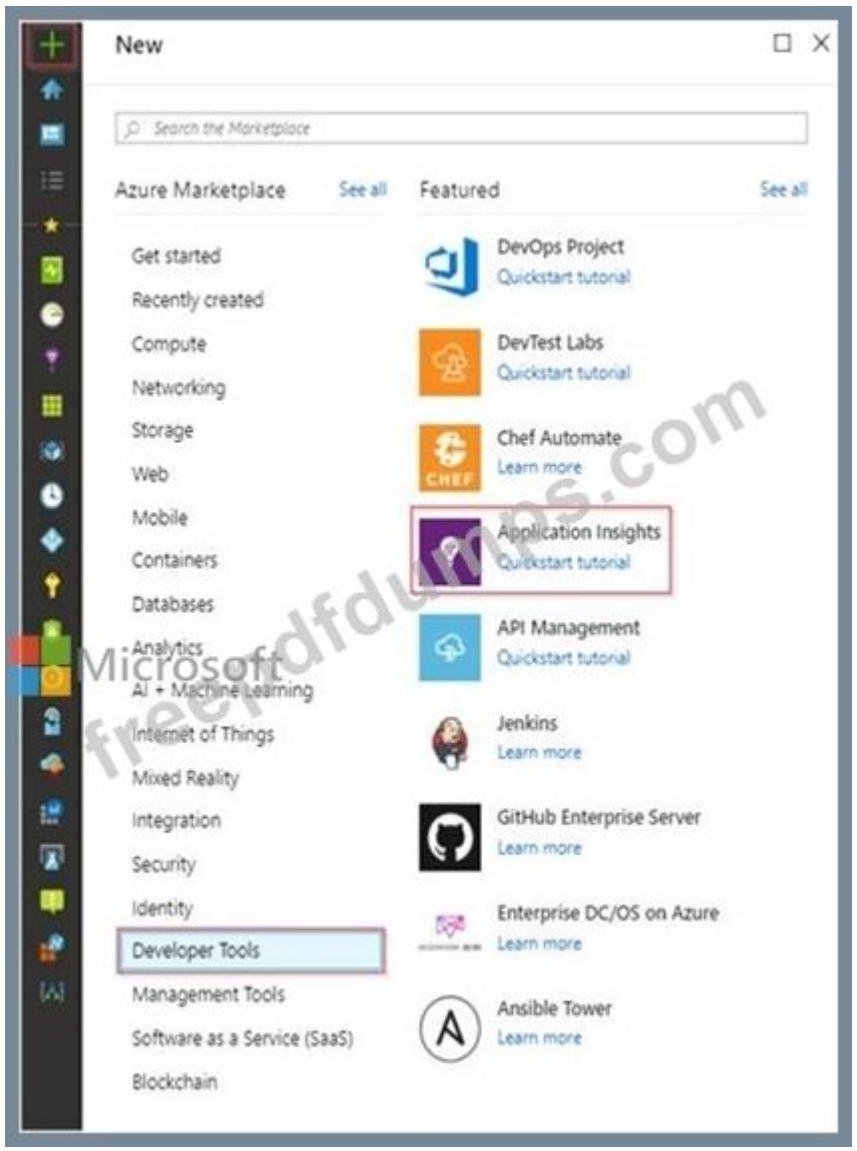
4. Open your ASP.NET Core Web App project in Visual Studio > Right-click on the AppName in the Solution Explorer > Select Add > Application Insights Telemetry.



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

B. Step 1: Create an instance of Azure Application Insights

1. Open Microsoft Azure Portal
2. Log into your Azure account, Select Create a resource > Developer tools > Application Insights.



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

Name: az400-9940427-main

Step 2: Configure App Insights SDK

4. Open your ASP.NET Core Web App project in Visual Studio > Right-click on the AppName in the Solution Explorer > Select Add > Application Insights Telemetry.

5. Click the Get Started button

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

Answer: A (LEAVE A REPLY)

References:

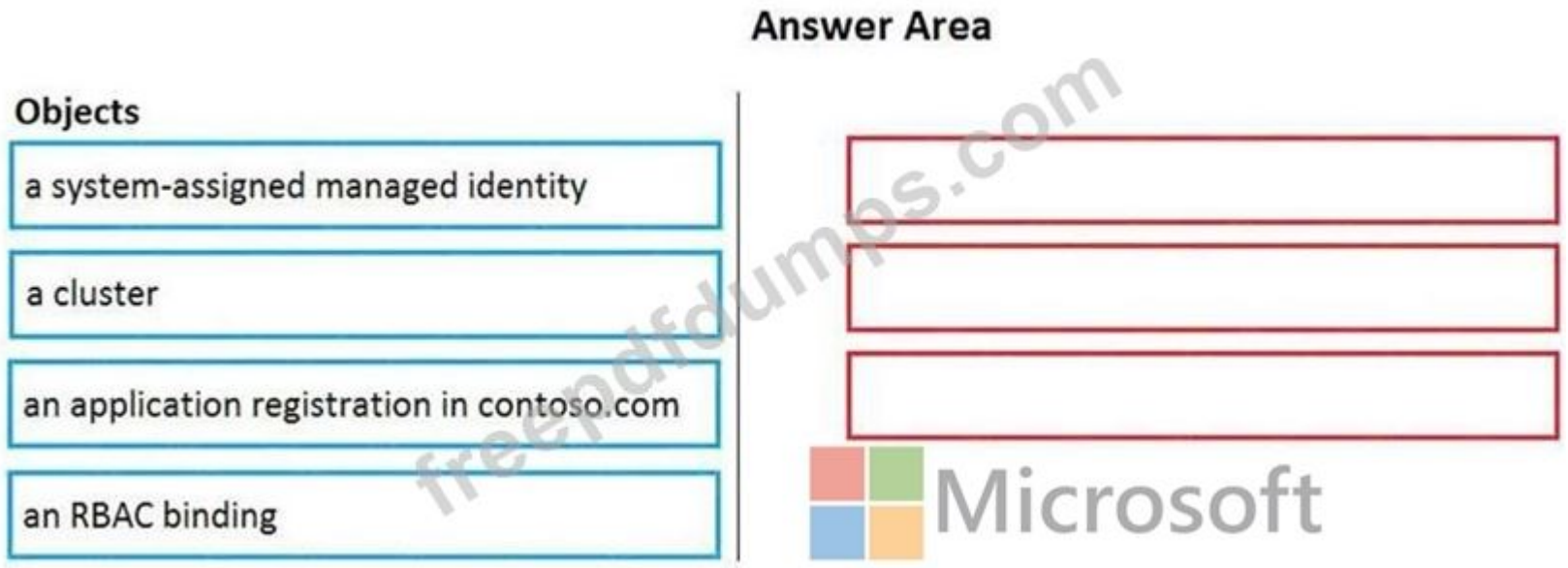
https://docs.microsoft.com/bs-latn-ba/azure/azure-monitor/learn/dotnetcore-quick-start?view=vs-2017

NEW QUESTION: 43

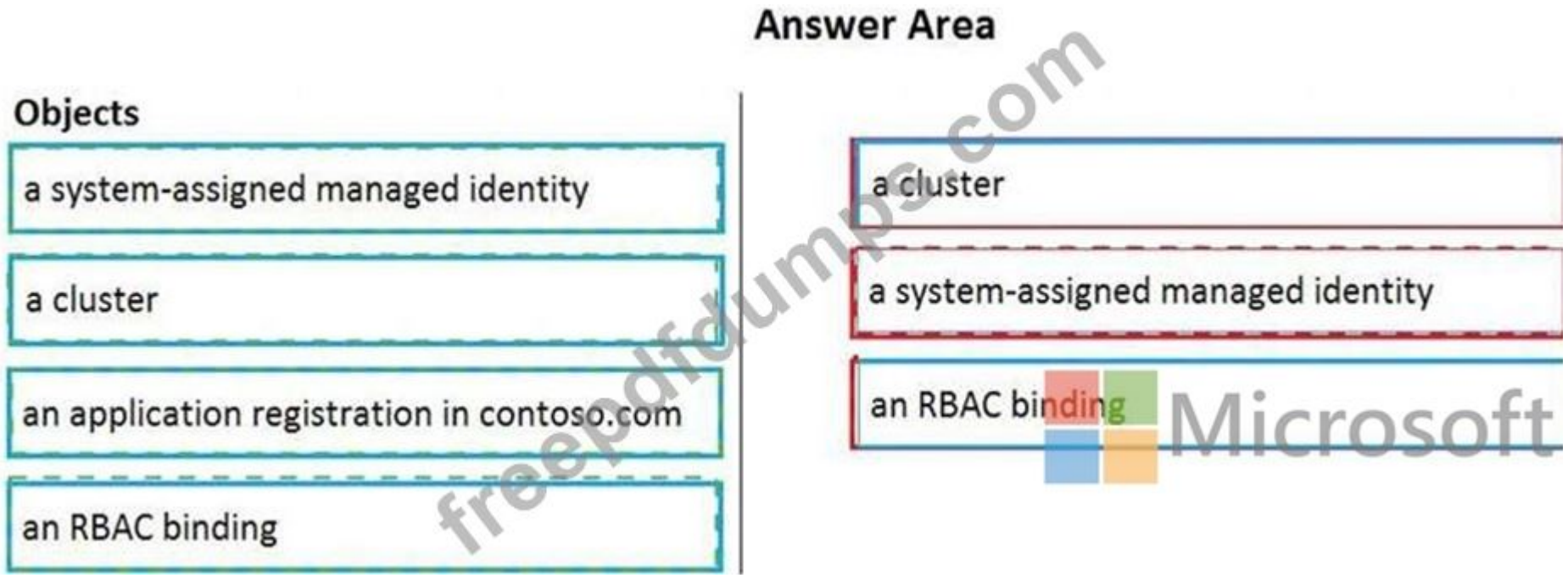
Your company has an Azure subscription named Subscription1. Subscription1 is associated to an Azure Active Directory tenant named contoso.com.

You need to provision an Azure Kubernetes Services (AKS) cluster in Subscription1 and set the permissions for the cluster by using RBAC roles that reference the identities in contoso.com.

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



Answer:



Explanation

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

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

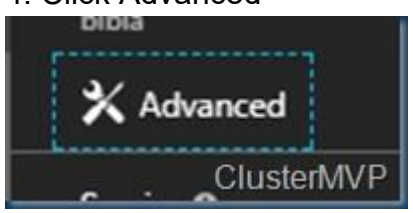
NEW QUESTION: 44
You manage the Git repository for a large enterprise application.
You need to minimize the data size of the repository.
How should you complete the commands? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation

Box 1: --aggressive
Cleanup unnecessary files and optimize the local repository:
git gc --aggressive
Box 2: prune
Prune all unreachable objects from the object database:
git prune
Reference:
https://gist.github.com/Zoramite/2039636

NEW QUESTION: 45
You need to prepare a network security group (NSG) named az400-9940427-nsg1 to host an Azure DevOps pipeline agent. The solution must allow only the required outbound port for Azure DevOps and deny all other inbound and outbound access to the Internet.
To complete this task, sign in to the Microsoft Azure portal.
Answer:
See solution below.
Explanation
1. Open Microsoft Azure Portal and Log into your Azure account.
2. Select network security group (NSG) named az400-9940427-nsg1
3. Select Settings, Outbound security rules, and click Add
4. Click Advanced



5. Change the following settings:
* Destination Port range: 8080
* Protocol. TCP
* Action: Allow
Note: By default, Azure DevOps Server uses TCP Port 8080.
References:
https://robertsmit.wordpress.com/2017/09/11/step-by-step-azure-network-security-groups-nsg-security-center-az
https://docs.microsoft.com/en-us/azure/devops/server/architecture/required-ports?view=azure-devops

NEW QUESTION: 46
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.

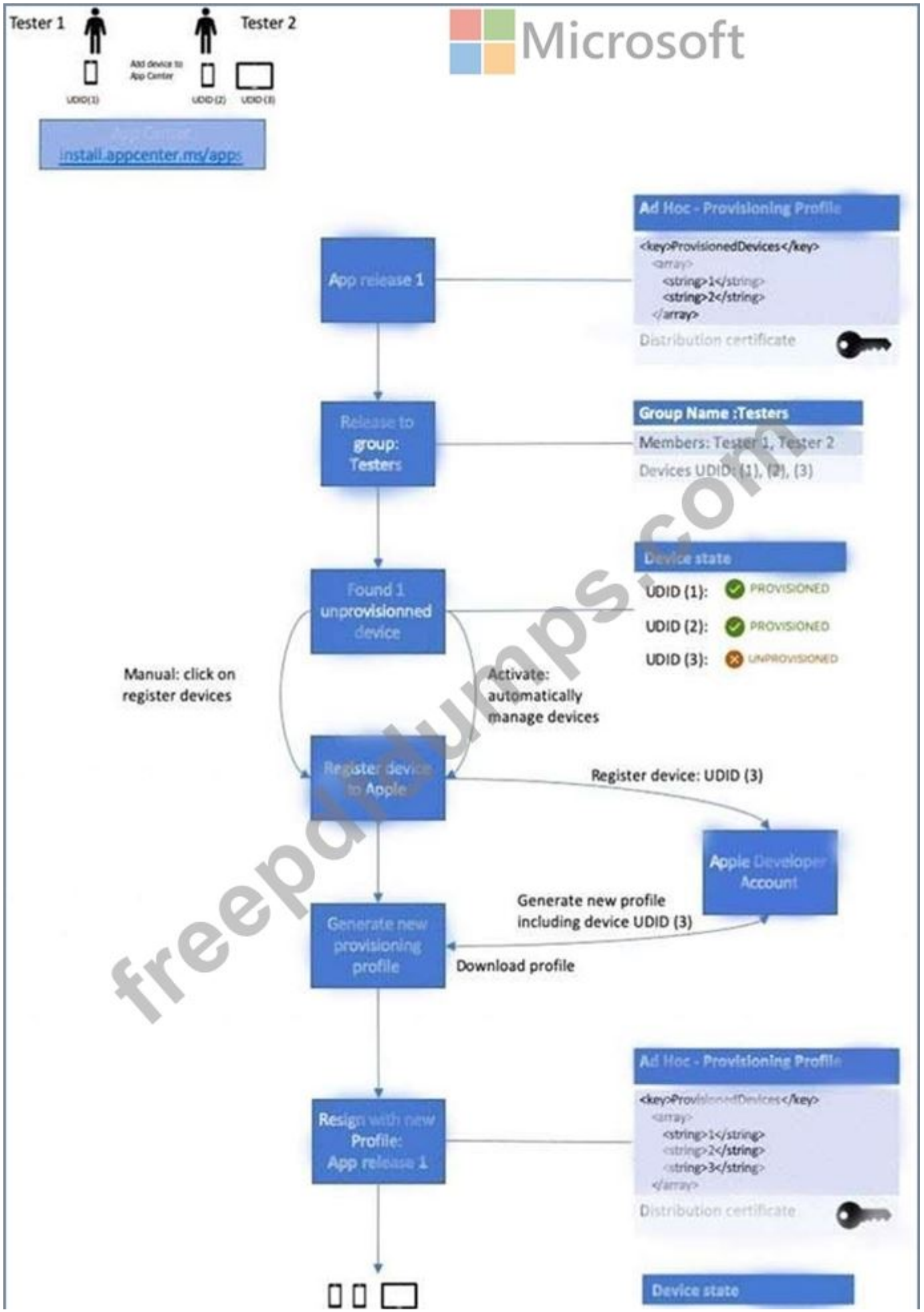
C. Create an active subscription in App Center Test.

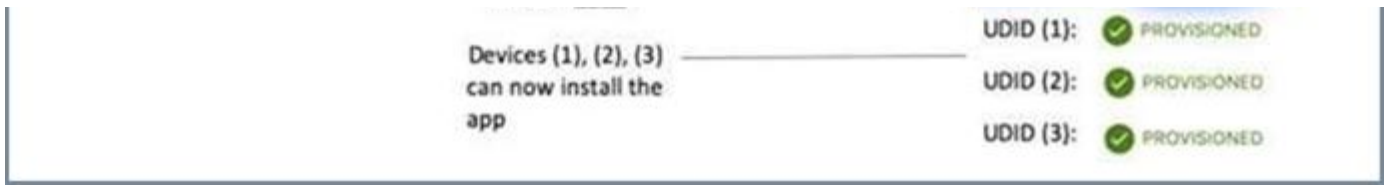
D. Add the device owner to the collaborators group.

Answer: A (LEAVE A REPLY)

Explanation

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



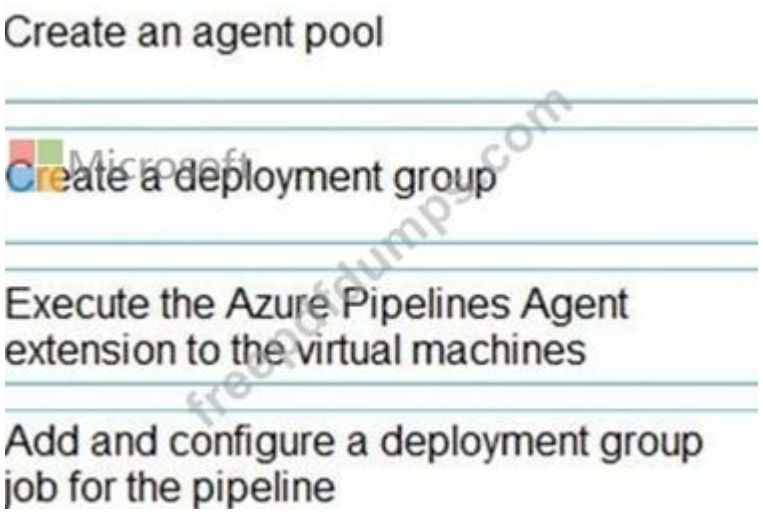


Reference:
https://docs.microsoft.com/hu-hu/appcenter/distribution/auto-provisioning

NEW QUESTION: 47
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 Information 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.

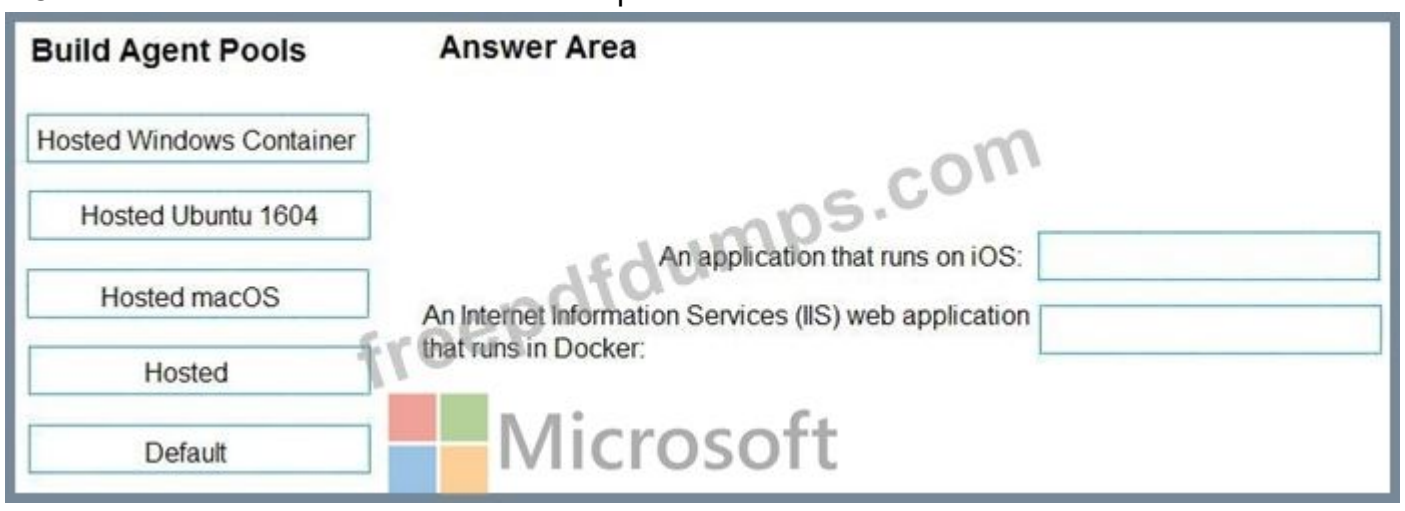
Answer:

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/howto-provision-deploymen

NEW QUESTION: 48
You mc configuring Azure DevOps build pipelines.
You plan to use hosted build agents.
Which build agent pool should you use to compile each application type? To answer, drag the appropriate built agent pools to the correct application types. Each butt agent pool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:

Explanation

Box 1: Hosted macOS

Hosted macOS pool (Azure Pipelines only): Enables you to build and release on macOS without having to configure a self-hosted macOS agent. This option affects where your data is stored.

Box 2: Hosted

Hosted pool (Azure Pipelines only): The Hosted pool is the built-in pool that is a collection of Microsoft-hosted agents.

NEW QUESTION: 49

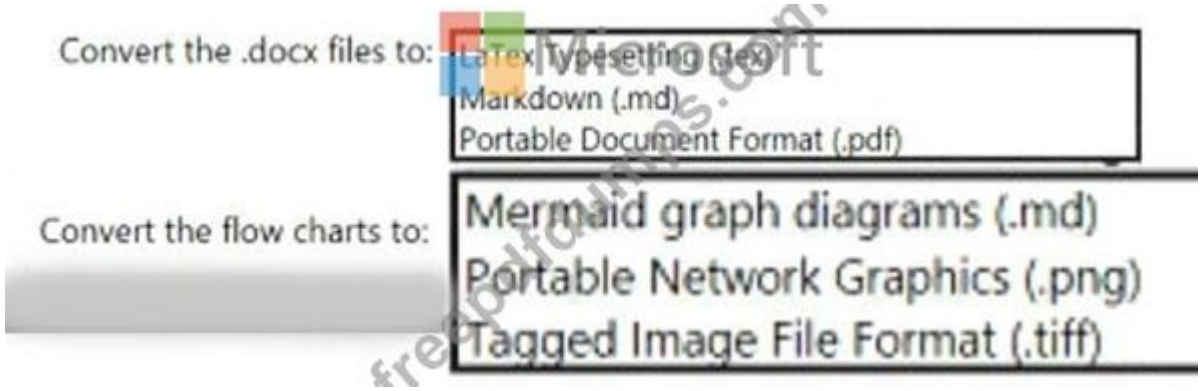
Your company uses GitHub for source control. GitHub repositories store source code and store process documentation. The process documentation is saved as Microsoft Word documents that contain simple flow charts stored as .bmp files.

You need to optimize the integration and versioning of the process documentation and the flow charts. The solution must meet the following requirements:

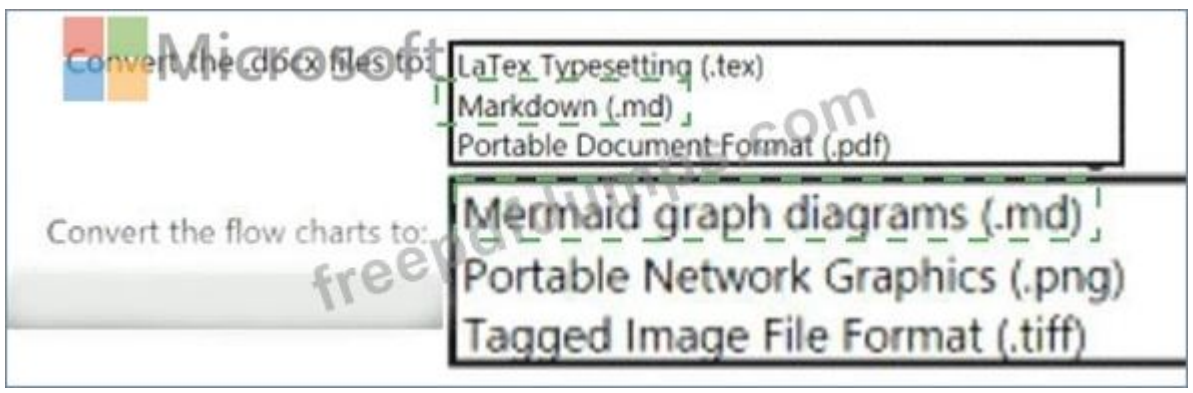
* Store documents as plain text.
* Minimize the number of files that must be maintained.
* Simplify the modification, merging, and reuse of flow charts.
* Simplify the modification, merging, and reuse of documents.

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:



NEW QUESTION: 50

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

You need to write ad-hoc Queries against the monitoring data.

Which Query language should you use?

A. PL/pgSQL

B. Transact-SQL

C. Azure Log Analytics

D. PL/SQL

Answer: (SHOW ANSWER)

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

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

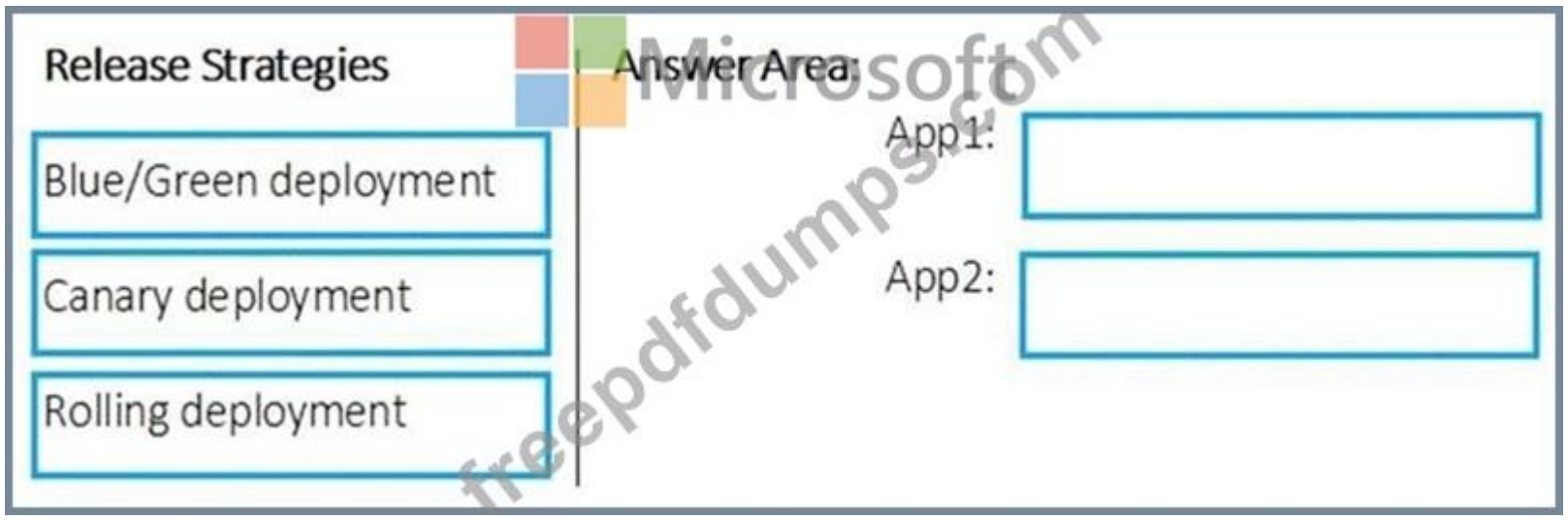
NEW QUESTION: 51

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

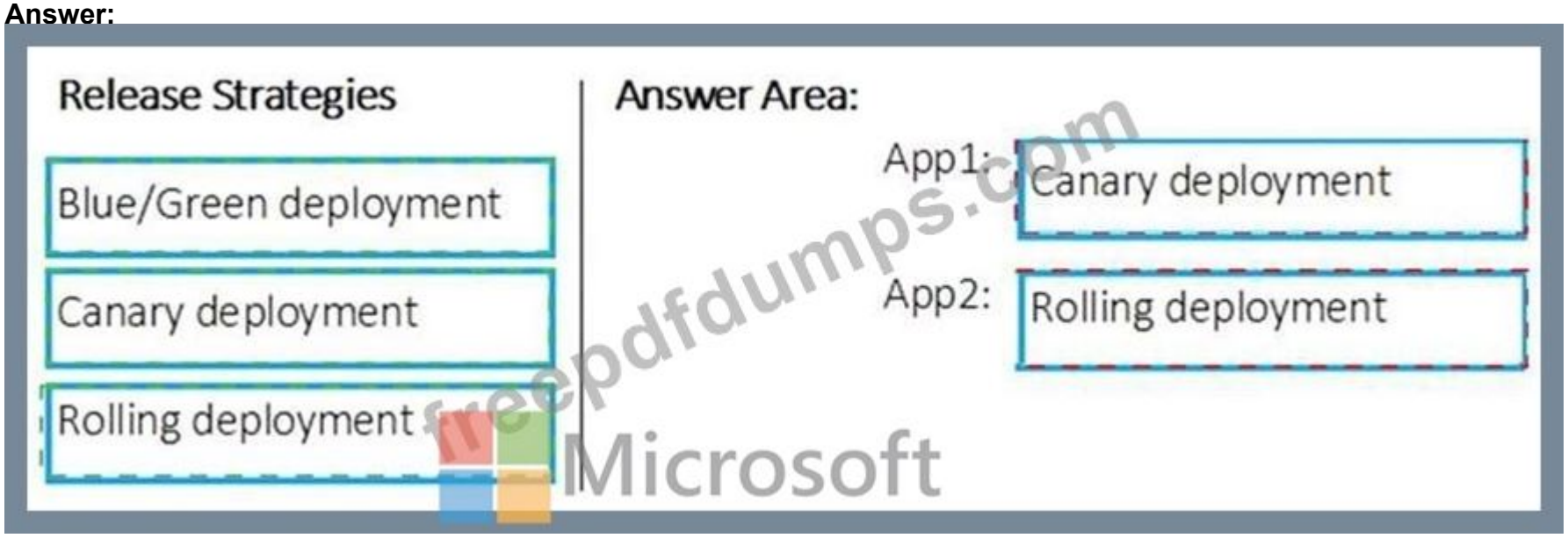
Application name	Goal
App1	Failure of App1 has a major impact on your company. You need a small group of users, who opted in to a testing App1, to test new releases of the application.
App2	You need to minimize the time it takes to deploy new releases of App2, and you must be able to roll back as quickly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

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

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



Answer:



Explanation

App1: Canary deployment
With canary deployment, you deploy a new application code in a small part of the production infrastructure.
Once the application is signed off for release, only a few users are routed to it. This minimizes any impact.
With no errors reported, the new version can gradually roll out to the rest of the infrastructure.
App2: Rolling deployment:
In a rolling deployment, an application's new version gradually replaces the old one. The actual deployment happens over a period of time. During that time, new and old versions will coexist without affecting functionality or user experience. This process makes it easier to roll back any new

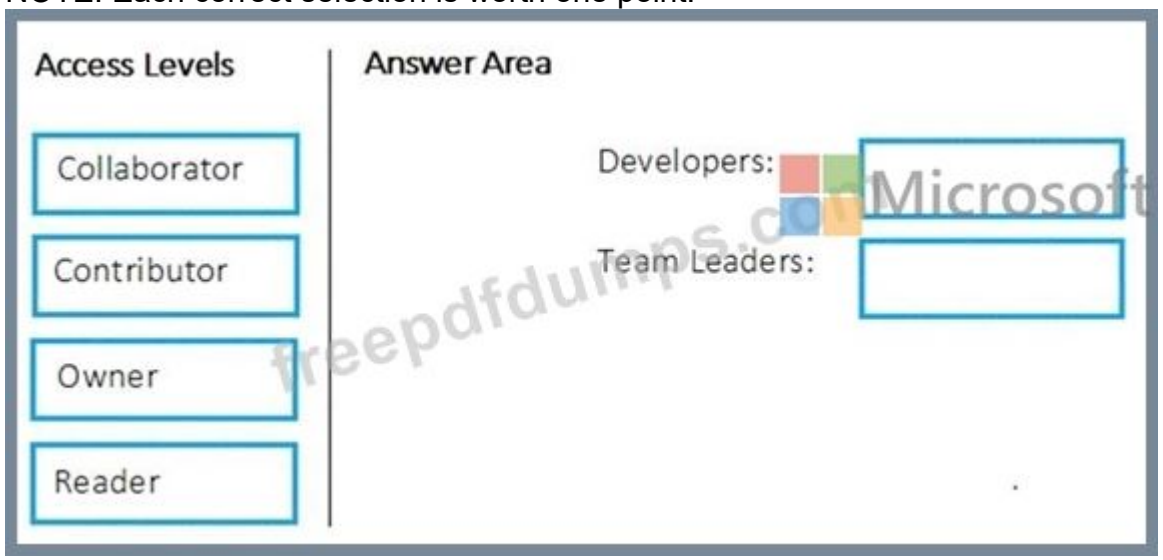
component incompatible with the old components.

NEW QUESTION: 52

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

Each access level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:

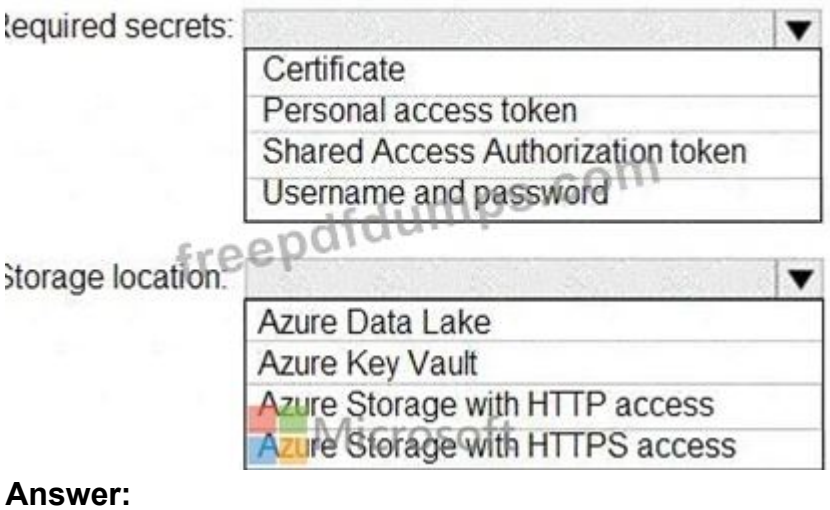
Explanation

Box 1: Reader

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

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

NEW QUESTION: 53
How should you confrere the release retention policy for the investment planning depletions suite? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation

Every request made against a storage service must be authorized, unless the request is for a blob or container resource that has been made available for public or signed access. One option for authorizing a request is by using Shared Key.

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

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

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

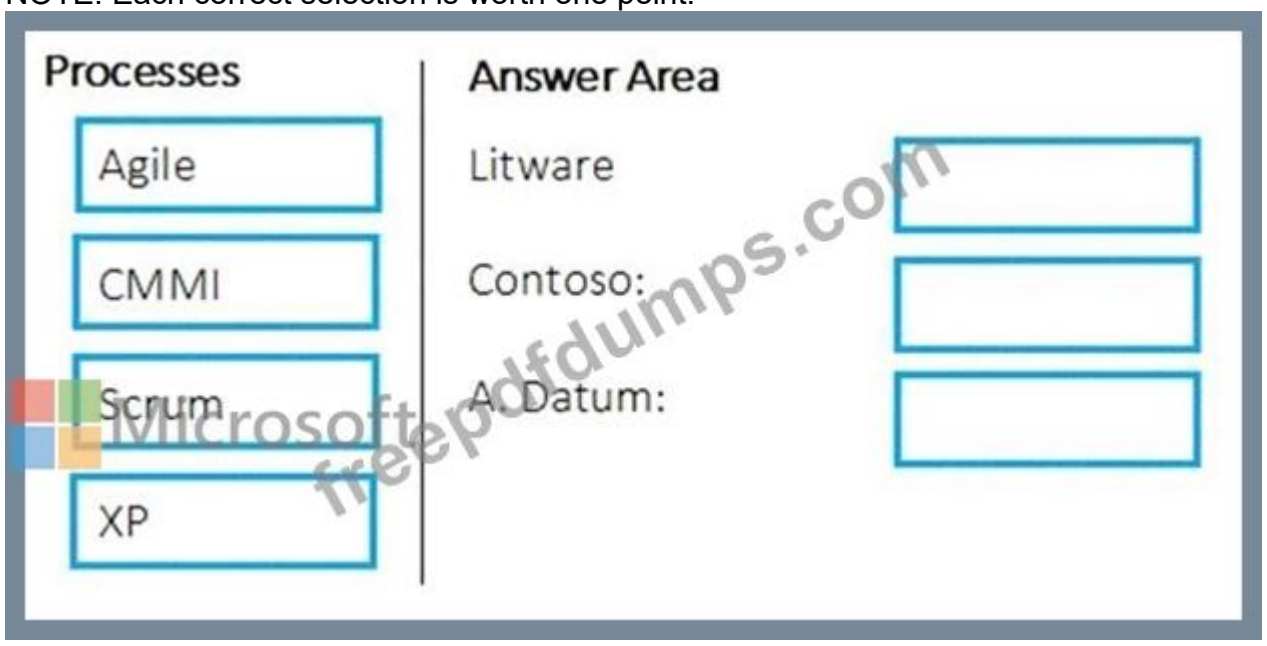
NEW QUESTION: 54

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

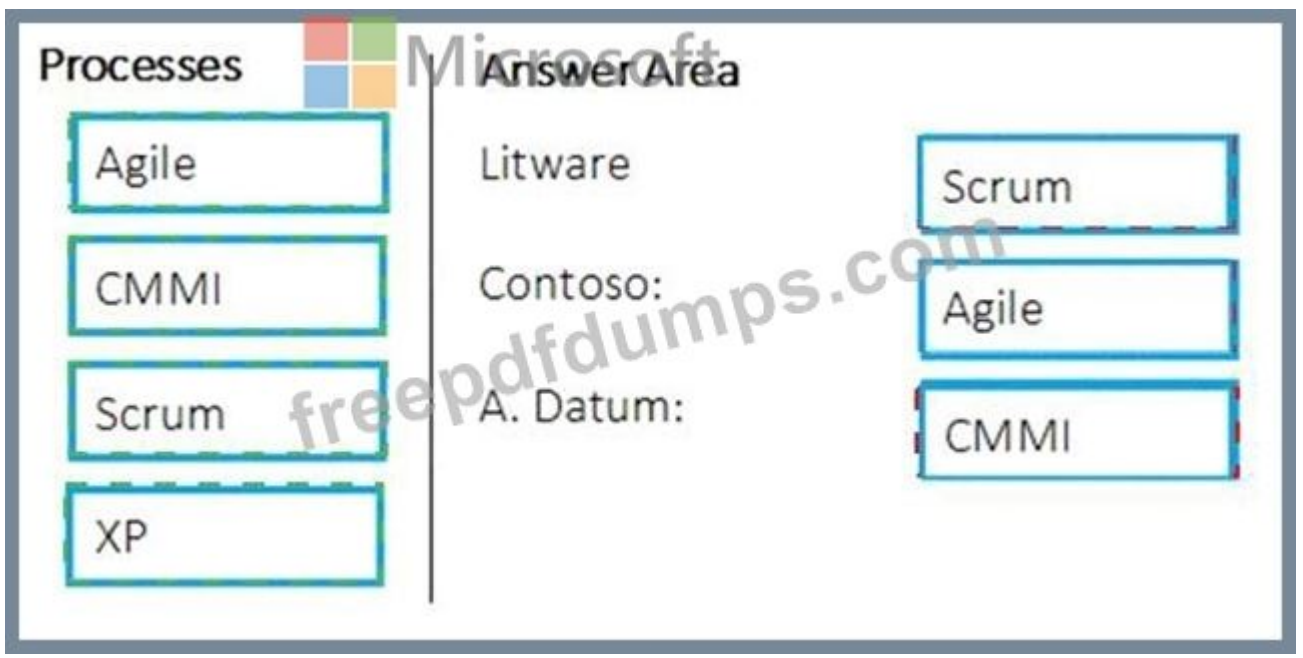
Customer name	Preferred process
Litware, Inc.	Track product backlog items (PBIs) and bugs on the Kanban board. Break the PBIs down into tasks on the task board.
Contoso, Ltd.	Track user stories and bugs on the Kanban board. Track the bugs and tasks on the task board.
A. Datum Corporation	Track requirements,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

The customers all plan to use Azure DevOps for work item management.

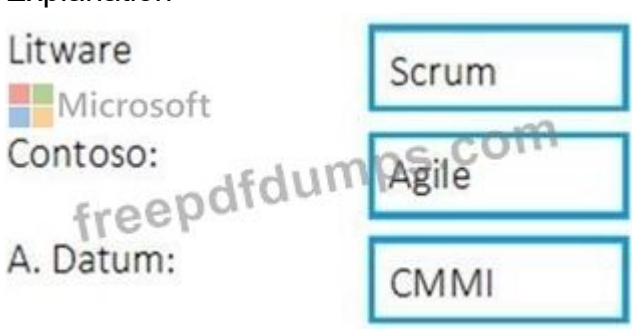
Which work item process should you use for each customer? To answer, drag the appropriate work item process to the correct customers. Each work item process may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:



Explanation



Box 1: Scrum
Choose Scrum when your team practices Scrum. This process works great if you want to track product backlog items (PBIs) and bugs on the Kanban board, or break PBIs and bugs down into tasks on the taskboard.

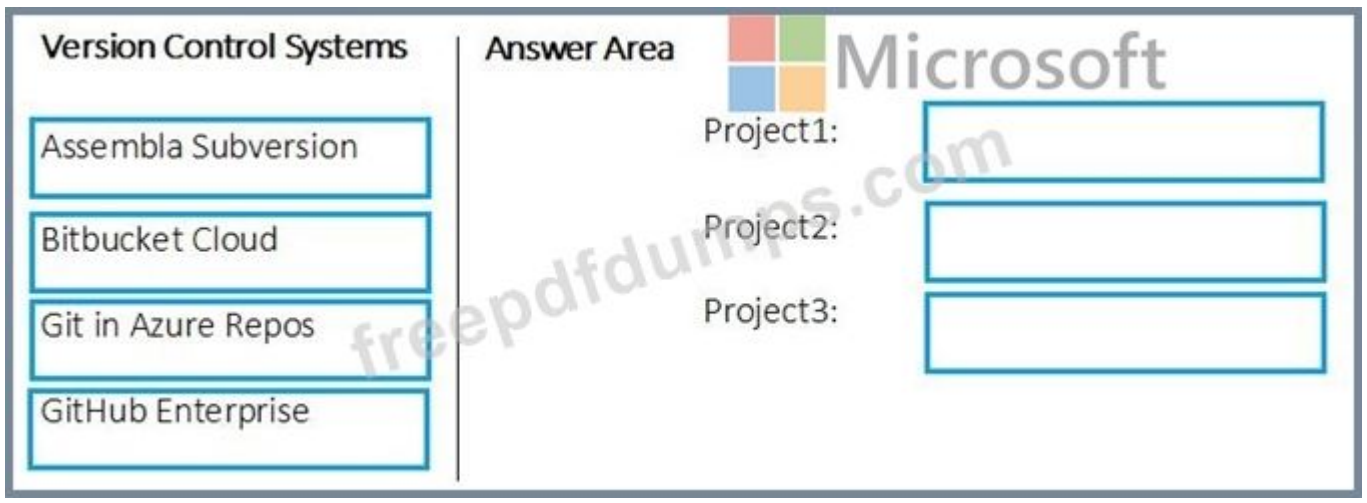
Box 2: Agile
Choose Agile when your team uses Agile planning methods, including Scrum, and tracks development and test activities separately. This process works great if you want to track user stories and (optionally) bugs on the Kanban board, or track bugs and tasks on the taskboard.
Box 3: CMMI
Choose CMMI when your team follows more formal project methods that require a framework for process improvement and an auditable record of decisions. With this process, you can track requirements, change requests, risks, and reviews.

NEW QUESTION: 55
Your company uses cloud-hosted Jenkins for builds.
You need to ensure that Jenkins can retrieve source code from Azure Repos.
Which three actions should you perform? Each correct answer presents part of the solution NOTE: Each correct answer selection is worth one point
A. Add the Team Foundation Server (TFS) plug-in to Jenkins.
B. Create a personal access token m your Azure DevOps account.
C. Create a webhook in Jenkins.
D. Add a domain to your Jenkins account.
E. Create a service hook m Azure DevOps.
Answer: A,B,E (LEAVE A REPLY)
Explanation
References:
https://blogs.msdn.microsoft.com/devops/2017/04/25/vsts-visual-studio-team-services-integration-with-jenkins/
http://www.aisoftwarellc.com/blog/post/how-to-setup-automated-builds-using-jenkins-and-visual-studio-team-fo

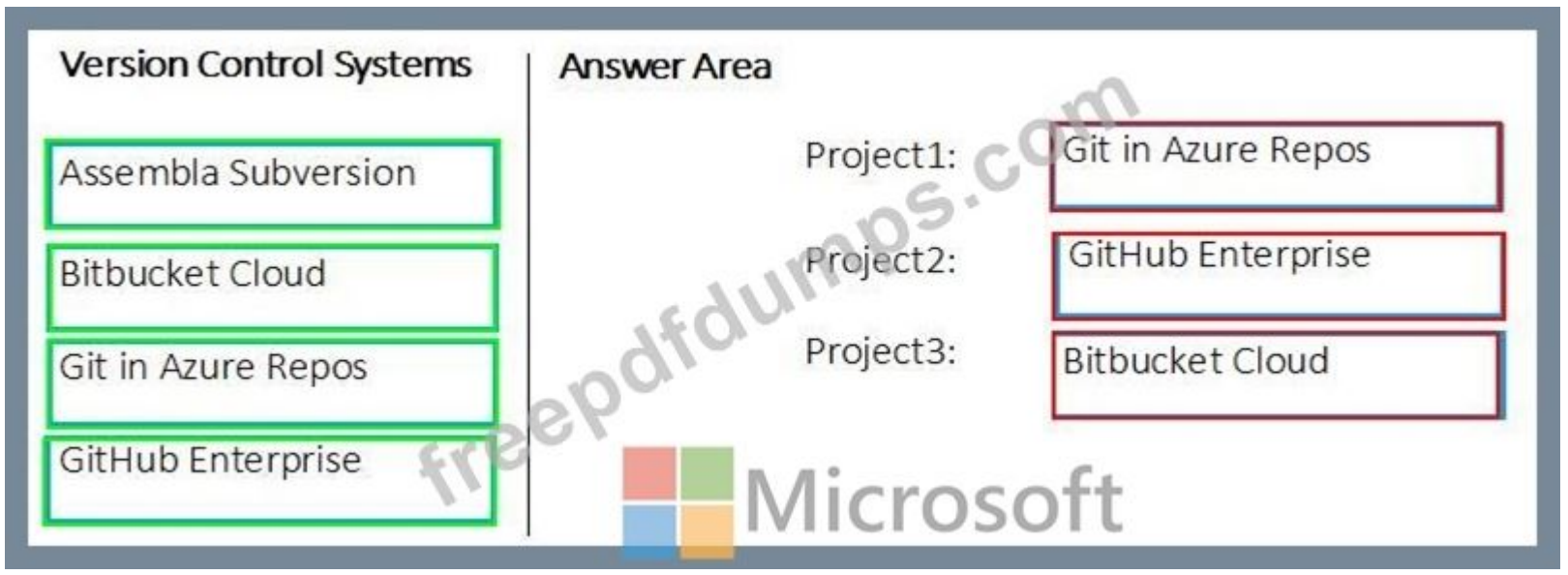
NEW QUESTION: 56
You are configuring Azure Pipelines for three projects in Azure DevOps as shown in the following table.

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.



Answer:



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.

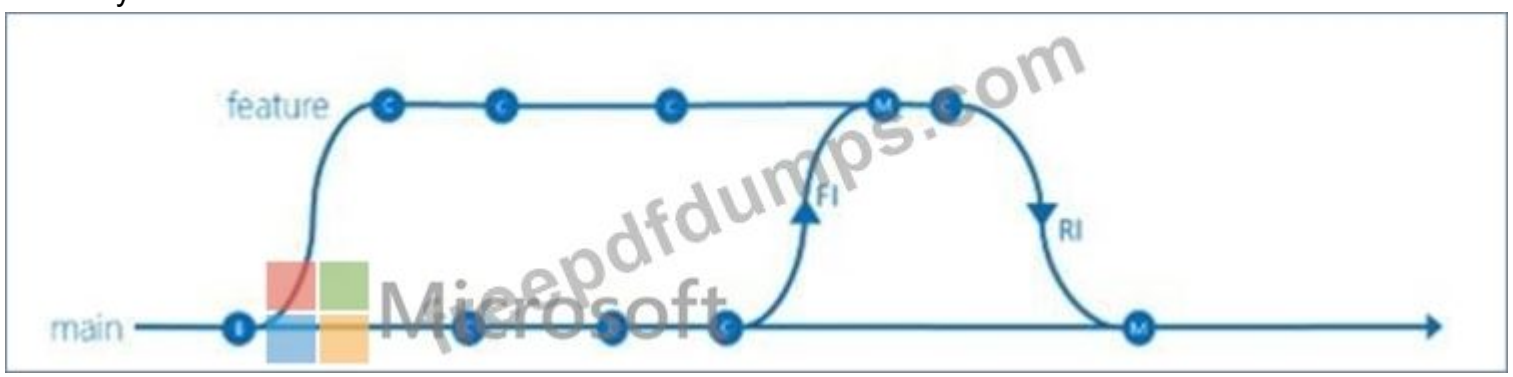
Note: A source control system, also called a version control system, allows developers to collaborate on code and track changes. Source control is an essential tool for multi-developer projects.

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:

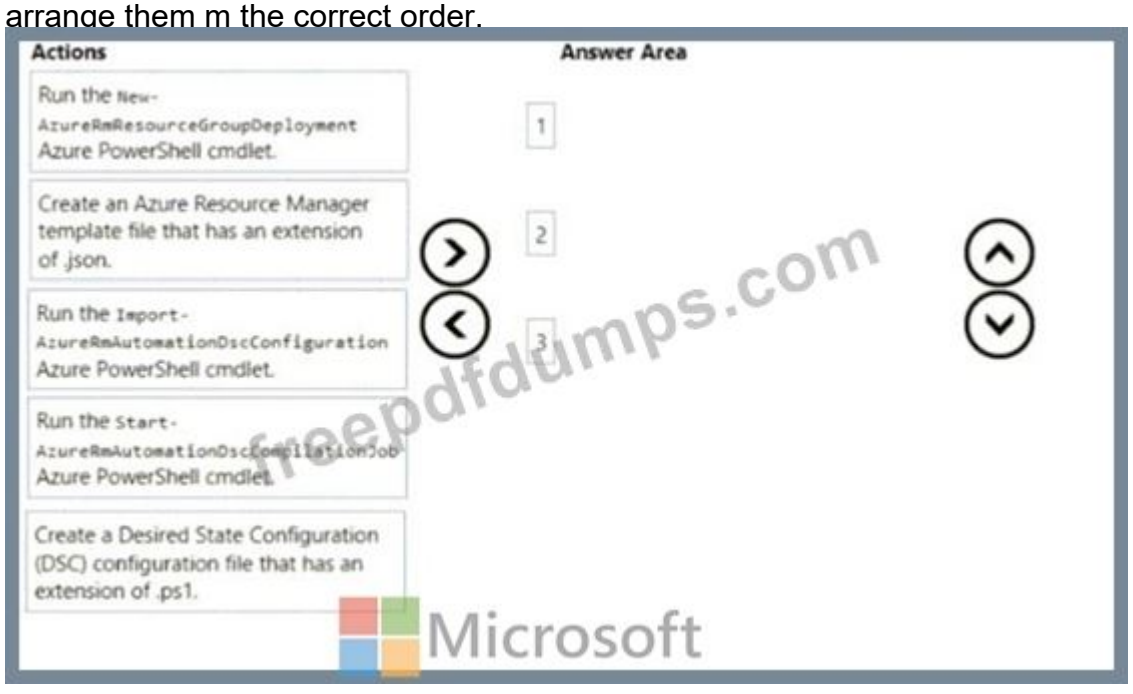
https://www.azuredevopslabs.com/labs/azuredevops/yaml/
https://enterprise.github.com/faq

NEW QUESTION: 57
Which branching strategy should you recommend for the investment planning applications suite?
A. release isolation
B. main only
C. development isolation
D. feature isolation
Answer: C (LEAVE A REPLY)
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.

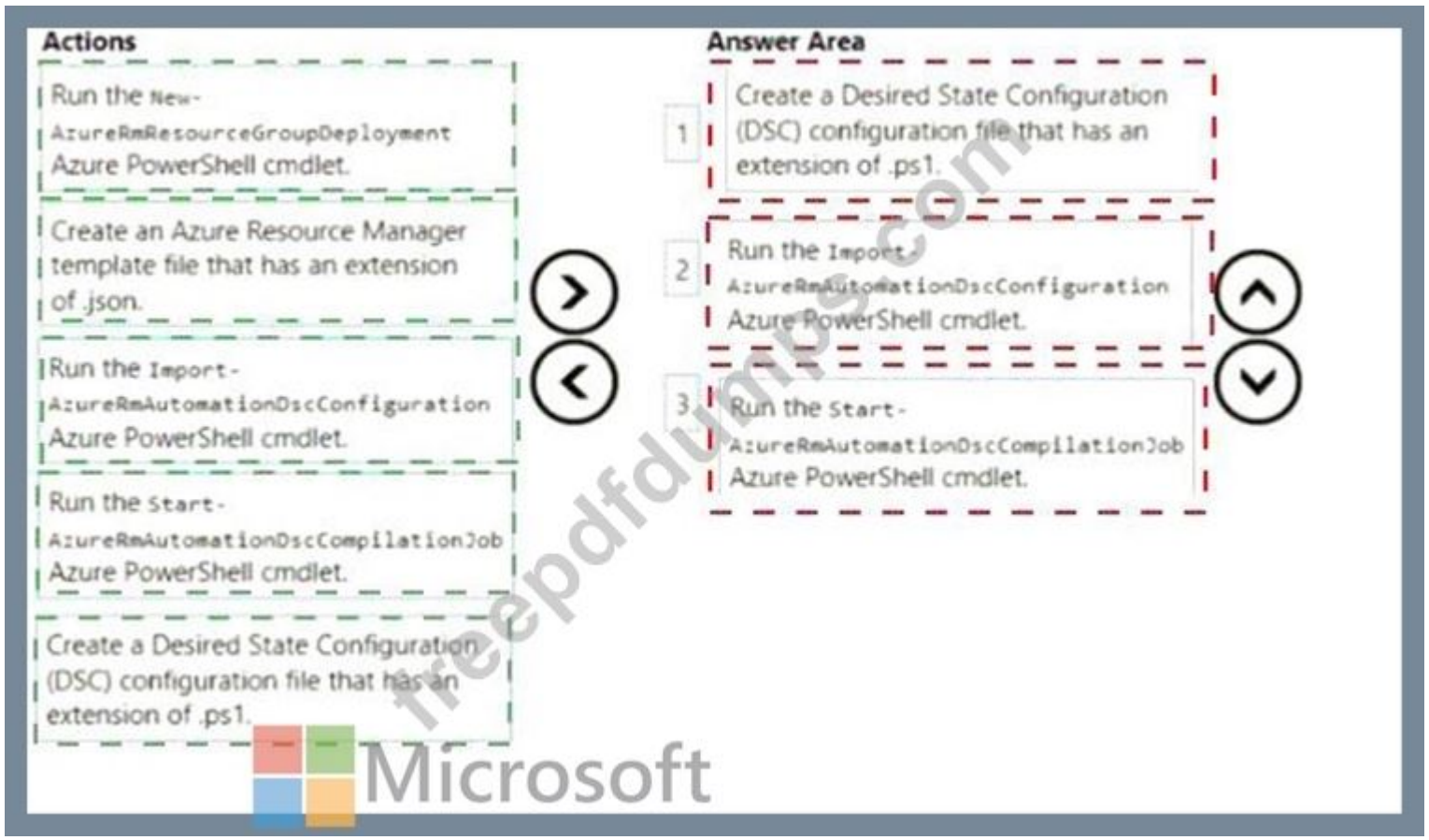


When you need to work on a particular feature, it might be a good idea to create a feature branch.

NEW QUESTION: 58
You need to configure Azure Automation for the computers in Pool7.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them m the correct order.



Answer:



Explanation

NEW QUESTION: 59

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: (SHOW ANSWER)

Explanation

https://github.com/dotnet/dotnet-docker/blob/master/samples/dotnetapp/README.md

NEW QUESTION: 60

You plan to deploy a template named D:\Deploy.json to a resource group named Deploy-lod9940427.

You need to modify the template to meet the following requirements, and then to deploy the template:

* The address space must be reduced to support only 256 total IP addresses.

* The subnet address space must be reduced to support only 64 total IP addresses.

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

Answer:

See solution below.

Explanation

1. Sign in to the portal,

2. Choose template Deploy-lod9940427

3. Select Edit template, and then paste your JSON template code into the code window.

4. Change the ASddressPrefixes to 10.0.0.0/24 in order to support only 256 total IP addresses.

addressSpace":{"addressPrefixes": ["10.0.0.0/24"]},

5. Change the firstSubnet addressprefix to 10.0.0.0/26 to support only 64 total IP addresses.

"subnets":[

{

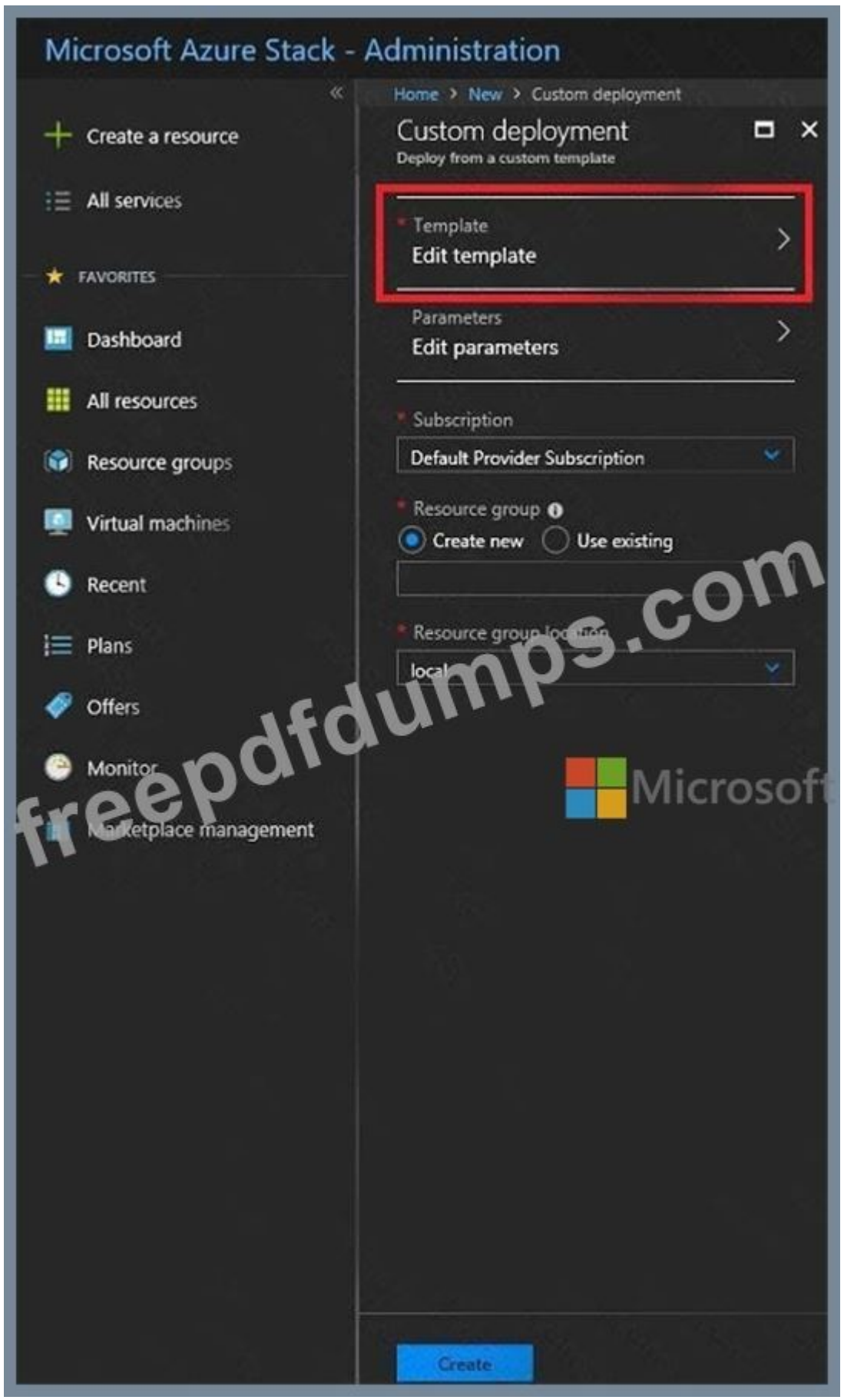
"name":"firstSubnet",

"properties":{

"addressPrefix":"10.0.0.0/24"

}

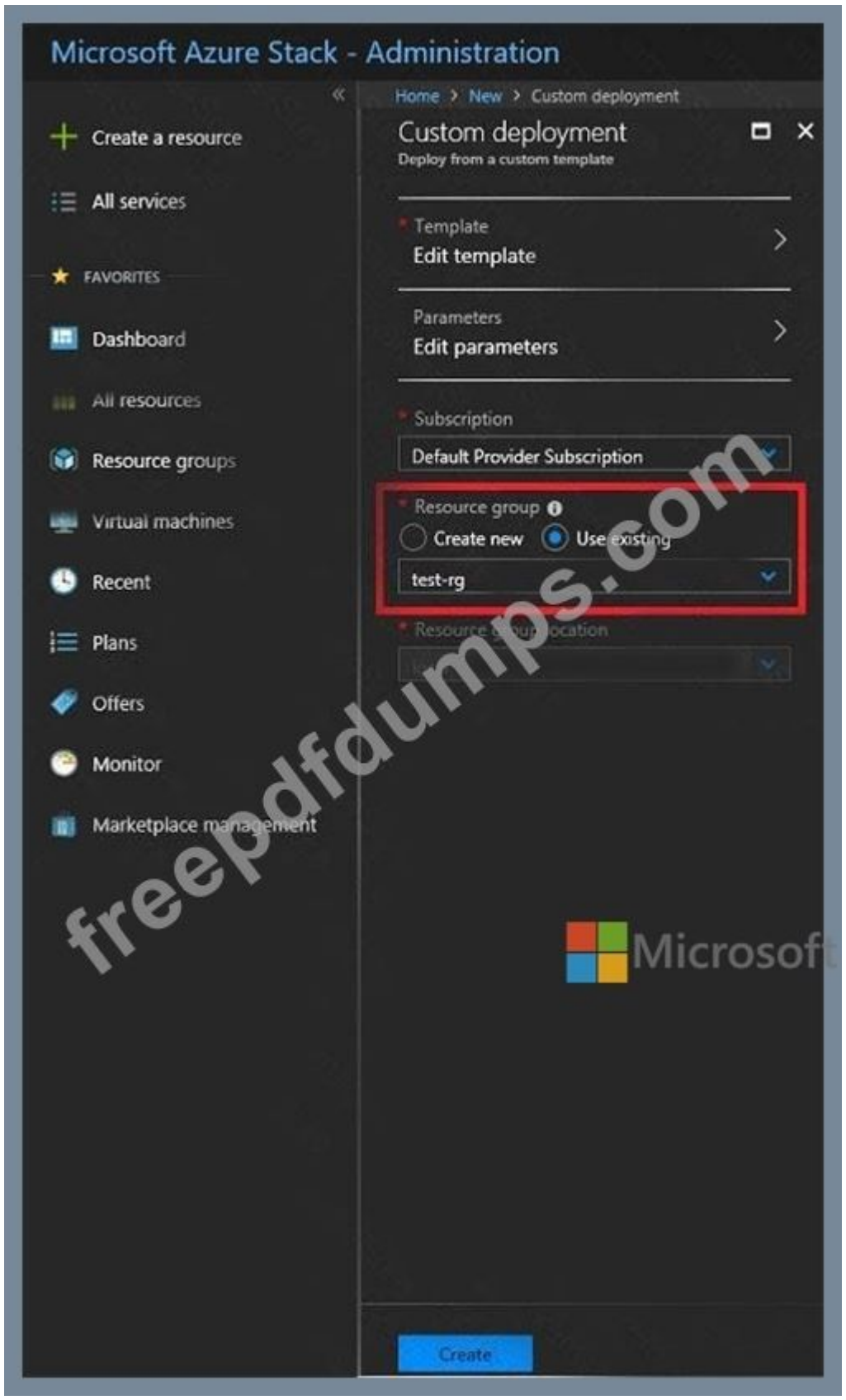
6. Select Save.



7. Select Edit parameters, provide values for the parameters that are shown, and then select OK.

8 Select Subscription. Choose the subscription you want to use, and then select OK.

9. Select Resource group. Choose an existing resource group or create a new one, and then select OK.



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

References:

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

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

NEW QUESTION: 61

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 Contoso project as shown in the Permissions exhibit (Click the Permissions tab.)

All other permissions have the default values set.

Answer:

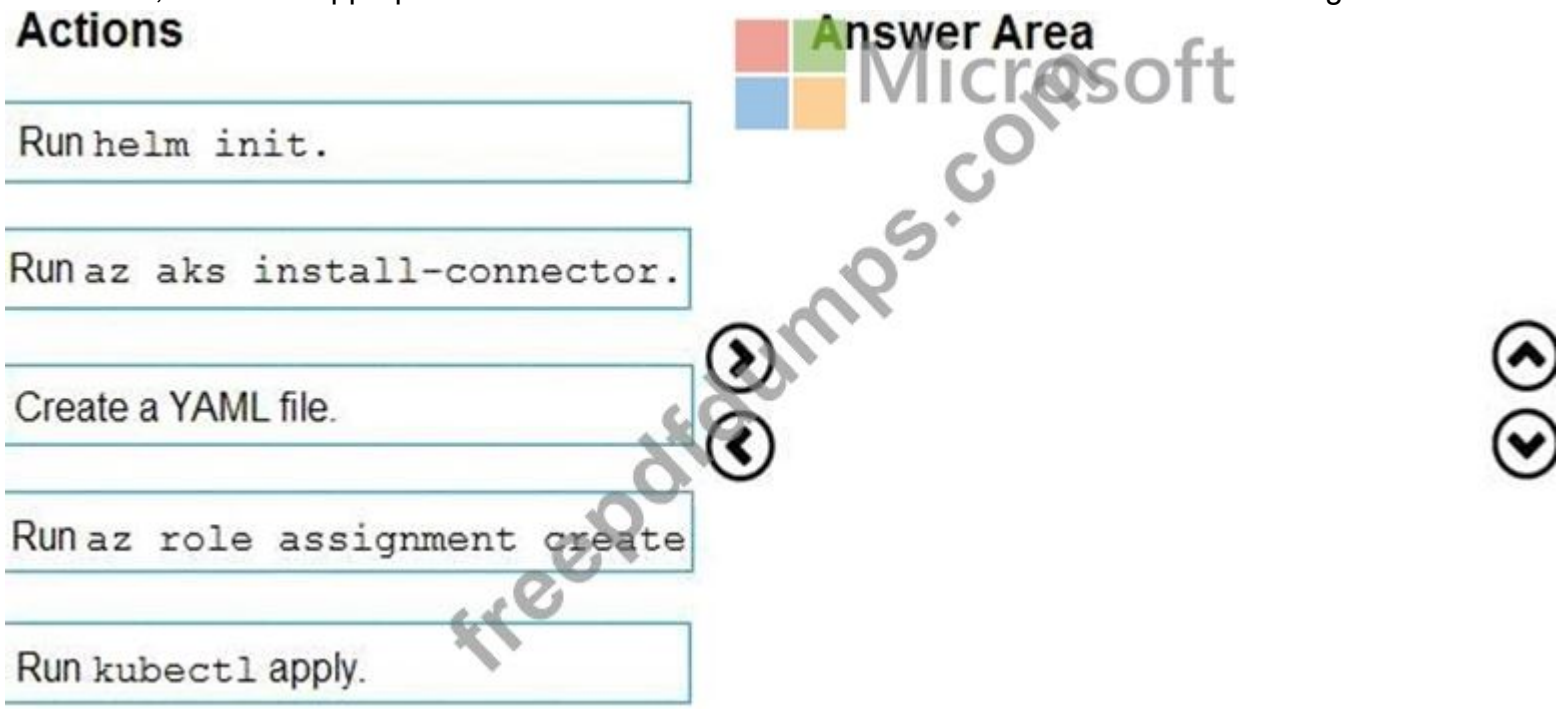
NEW QUESTION: 62

You have an Azure Kubermets Service (AKS) implementation that is RBAC-enabled You plan to use Azure Container Instances as a hosted development environment to run containers in the AKS implementation.

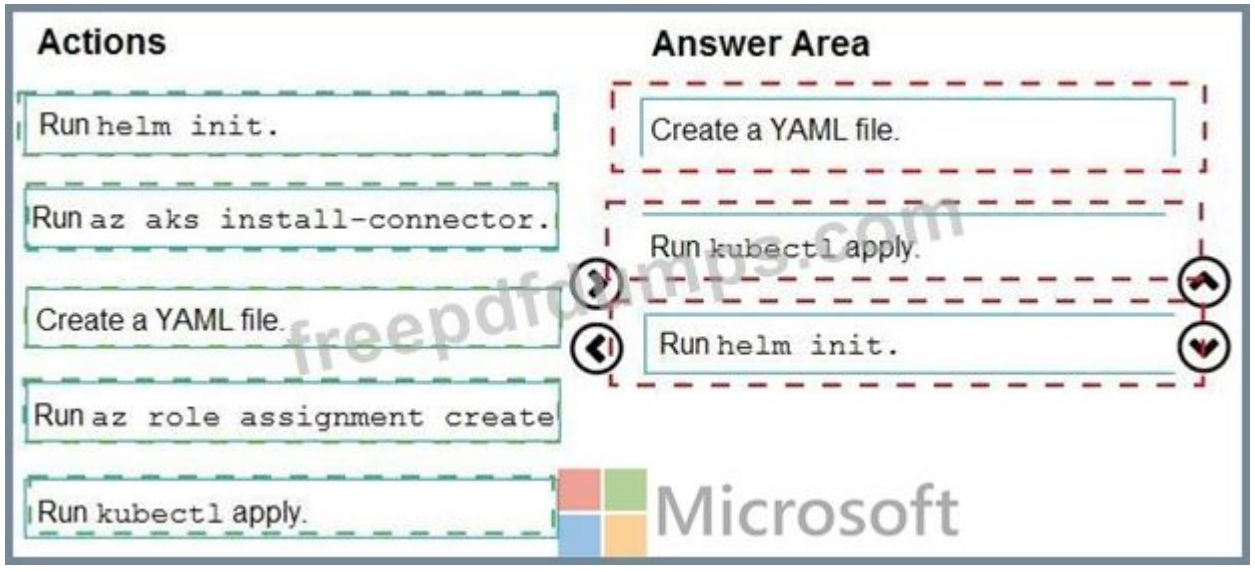
You need to conjure Azure Container Instances as a hosted environment for running me containers in AKS.

Which three actions should you perform m sequence?

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



Answer:

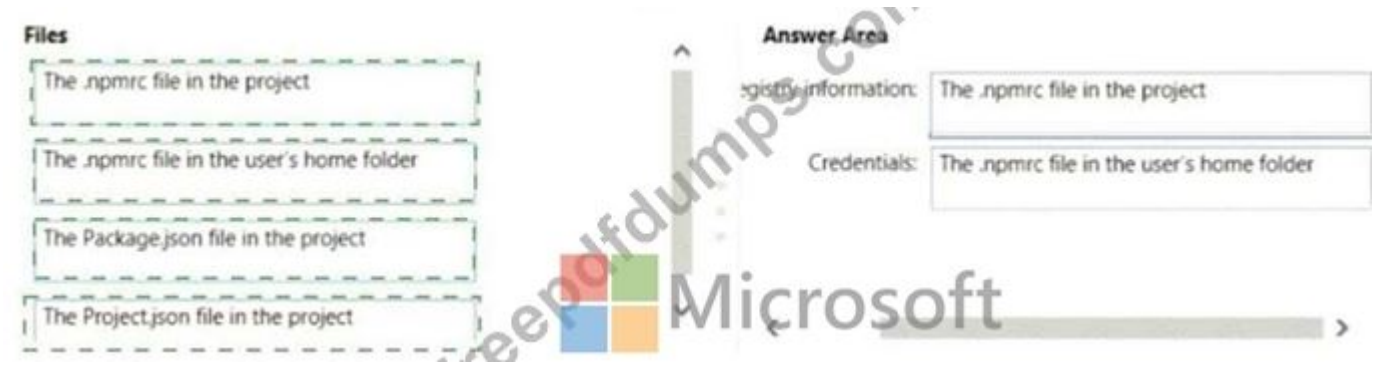


Explanation

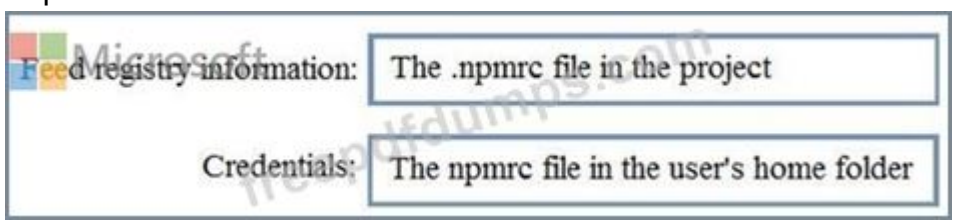
Step 1: Create a YAML file.
If your AKS cluster is RBAC-enabled, you must create a service account and role binding for use with Tiller.
To create a service account and role binding, create a file named rbac-virtual-kubelet.yaml Step 2: Run kubectl apply.
Apply the service account and binding with kubectl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

NEW QUESTION: 63
You are implementing a package management solution for a Node.js application by using Azure Artifacts.
You need to configure the development environment to connect to the package repository. The solution must minimize the likelihood that credentials will be leaked.
Which file should you use to configure each connection? To answer, drag the appropriate files to the correct connections. Each file may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content NOTE: Each correct selection is worth one point.

Answer:



Explanation



All Azure Artifacts feeds require authentication, so you'll need to store credentials for the feed before you can install or publish packages. npm uses .npmrc configuration files to store feed URLs and credentials. Azure DevOps Services recommends using two .npmrc files.

Feed registry information: The .npmrc file in the project

One .npmrc should live at the root of your git repo adjacent to your project's package.json. It should contain a "registry" line for your feed and it should not contain credentials since it will be checked into git.

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

On your development machine, you will also have a .npmrc in $home for Linux or Mac systems or $env.HOME for win systems. This .npmrc should contain credentials for all of the registries that you need to connect to. The NPM client will look at your project's .npmrc, discover the registry, and fetch matching credentials from $home/.npmrc or $env.HOME/.npmrc.

References:

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

NEW QUESTION: 64

Note: This question n part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution After you answer a question in this section, you will NOT be able to return to it. As a result these questions will not appear in the review screen.

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

You have a policy stating that approvals must occur within eight hours.
You discover that deployments fail if the approvals lake longer than two hours.
You need to ensure that the deployments only fail if the approvals take longer than eight hours.
Solution: From Pre-deployment conditions, you modify the Timeout setting for pre-deployment approvals.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
Explanation
Use a gate instead of an approval instead.
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates

NEW QUESTION: 65
You add the virtual machines as managed nodes in Azure Automation State Configuration.
You need to configure the computers in Group7.
What should you do?
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 (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The Register-AzureRmAutomationDscNode cmdlet registers an Azure virtual machine as an APS Desired State Configuration (DSC) node in an Azure Automation account.
Scenario: The Azure DevOps organization includes:
The Docker extension
A deployment pool named Pool7 that contains 10 Azure virtual machines that run Windows Server 2016

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

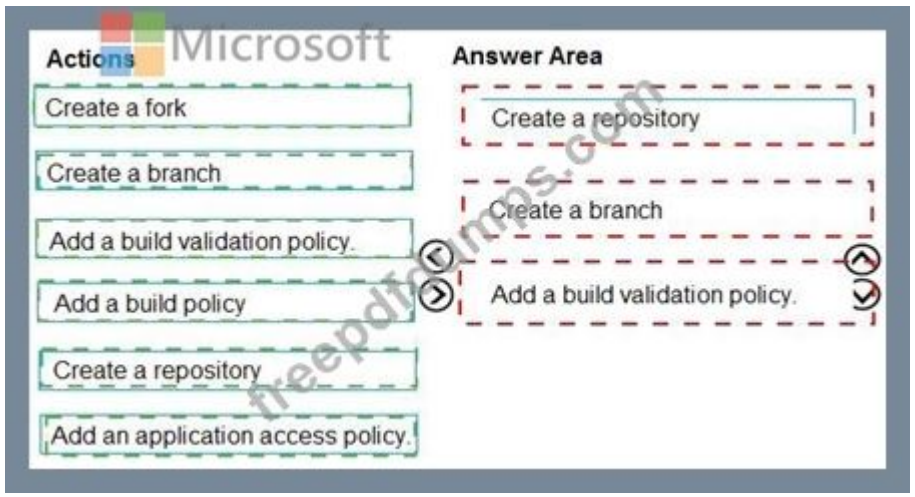
References: https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register- azurermautomationdscnode Question Set 3

NEW QUESTION: 66
You have an Azure function hosted in an App Service plan named az400-9940427-func1.
You need to configure az400-9940427-func1 to upgrade the functions automatically whenever new code is committed to the master branch of https://github.com/Azure-Samples/functions-quickstart.
To complete this task, sign in to the Microsoft Azure portal.
A. 1. Open Microsoft Azure Portal
2. Log into your Azure account, select App Services in the Azure portal left navigation, and then select configure az400-9940427-func1.
3. On the app page, select Deployment Center in the left menu.
4. On the Build provider page, select Azure Pipelines (Preview), and then select Continue.

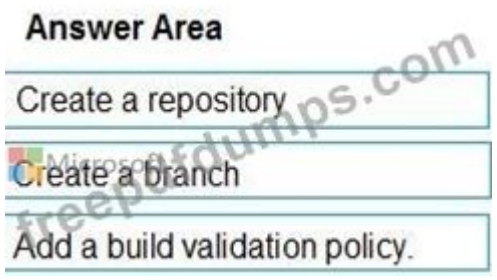
5. On the Configure page, in the Code section:
For GitHub, drop down and select the Organization, Repository, and Branch you want to deploy continuously.
6. Select Continue.
7. On the Test page, choose whether to enable load tests, and then select Continue.
8. Depending on your App Service plan pricing tier, you may see a Deploy to staging page. Choose whether to enable deployment slots, and then select Continue.
9. After you configure the build provider, review the settings on the Summary page, and then select Finish.
B. 1. Open Microsoft Azure Portal
2. Log into your Azure account, select App Services in the Azure portal left navigation, and then select configure az400-9940427-func1.
3. On the app page, select Deployment Center in the left menu.
4. On the Build provider page, select Azure Pipelines (Preview), and then select Continue.
5. On the Configure page, in the Code section:
For GitHub, drop down and select the Organization, Repository, and Branch you want to deploy continuously.
6. Select Continue.
7. Depending on your App Service plan pricing tier, you may see a Deploy to staging page. Choose whether to enable deployment slots, and then select Continue.
8. After you configure the build provider, review the settings on the Summary page, and then select Finish.
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/app-service/deploy-continuous-deployment

NEW QUESTION: 67
You need to implement the code flow strategy for Project2 in Azure DevOps.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange in the correct order.

Answer:



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

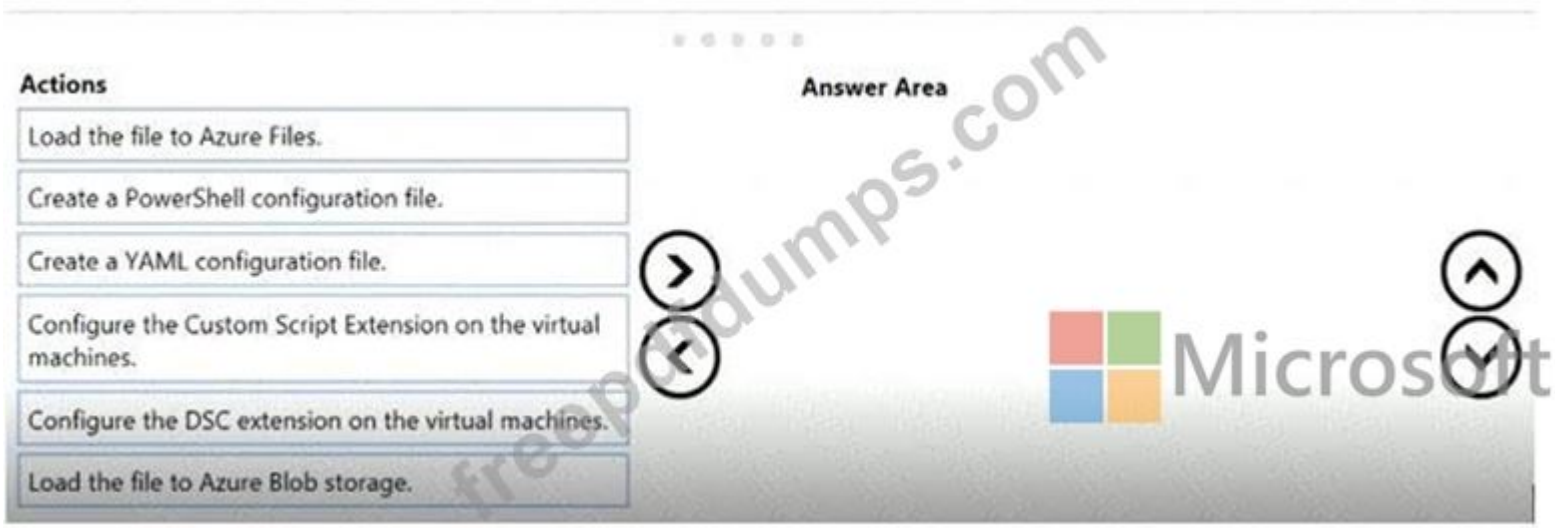
NEW QUESTION: 68

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

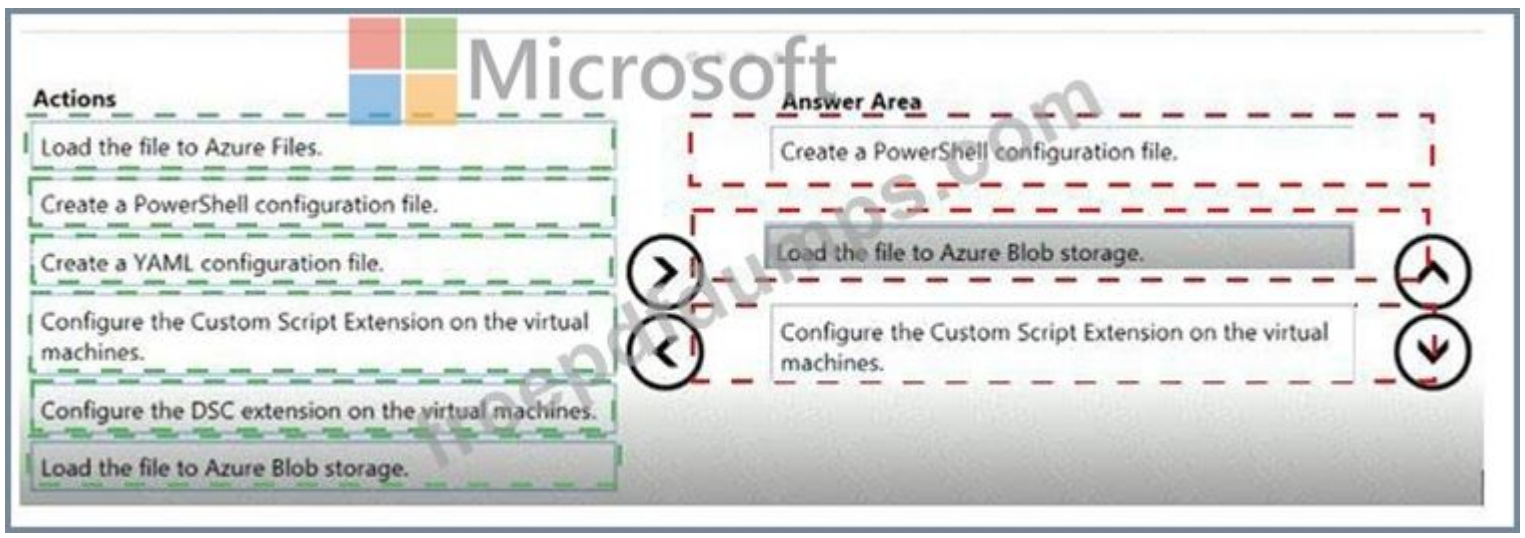
You plan to use the Desired State Configuration (DSC) extension on the virtual machines.

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

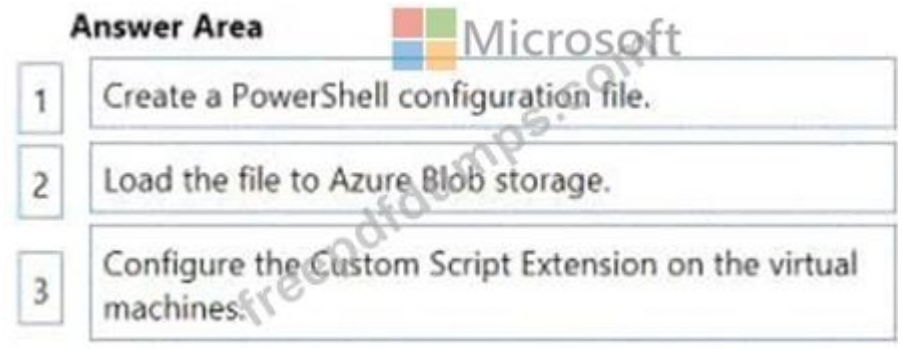
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



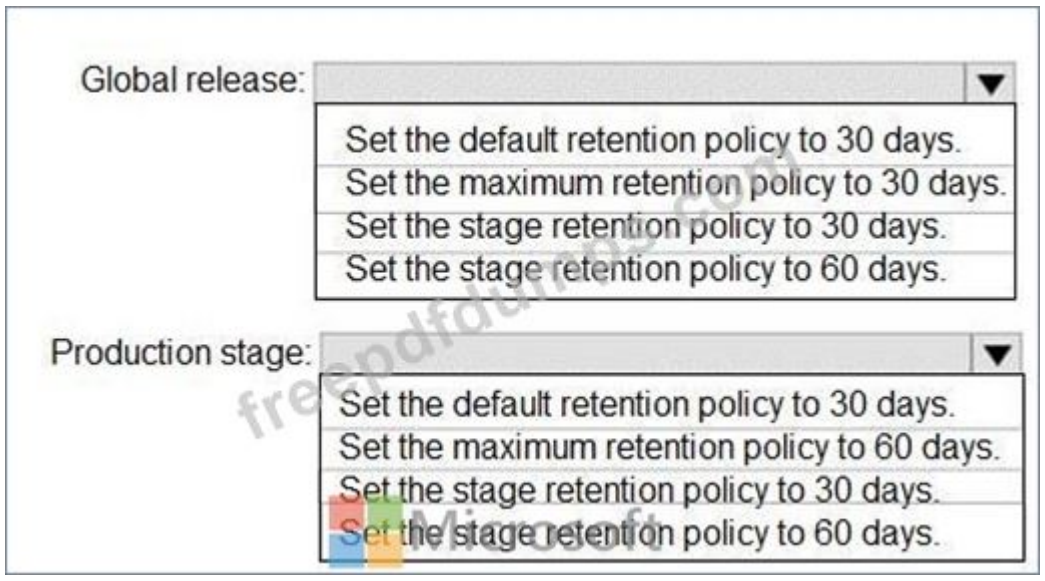
Explanation



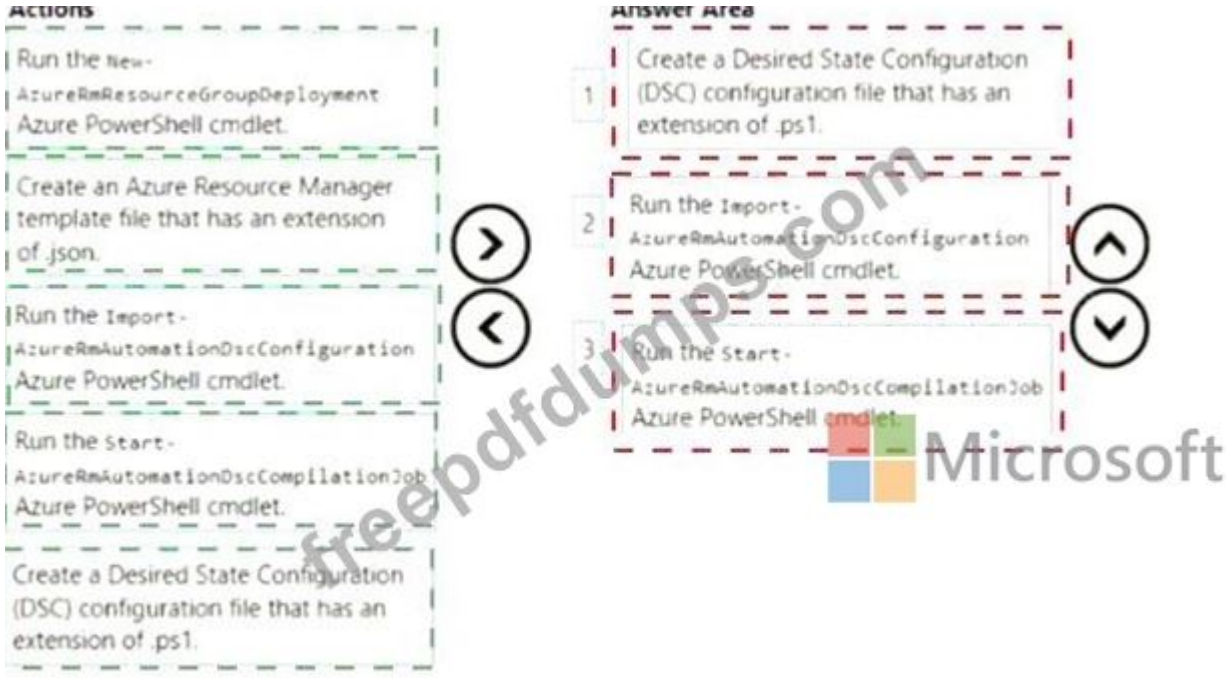
NEW QUESTION: 69

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

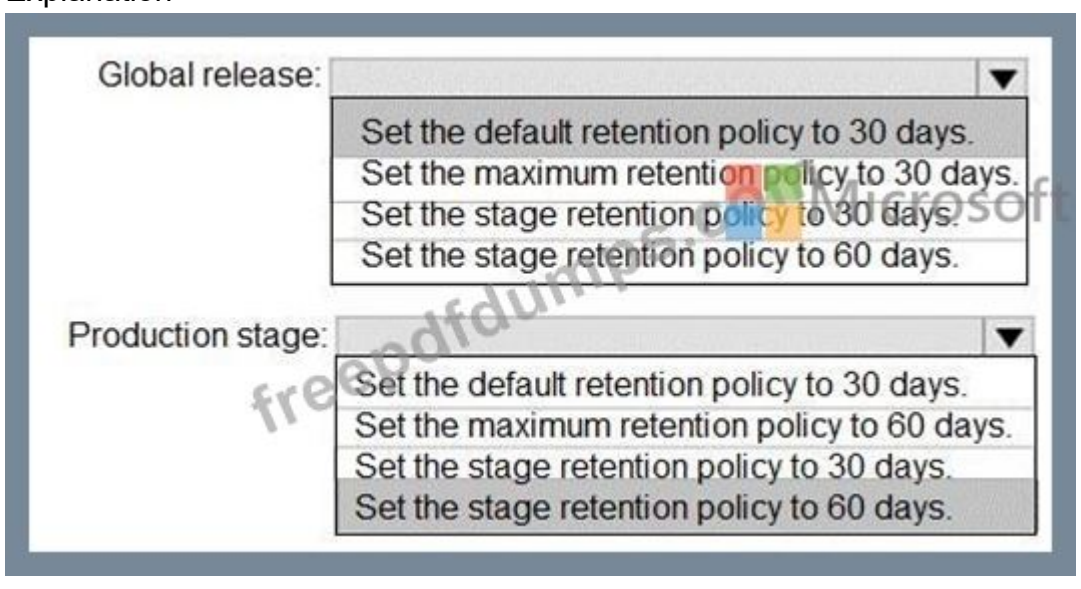
NOTE: Each correct selection is worth one point.



Answer:



Explanation



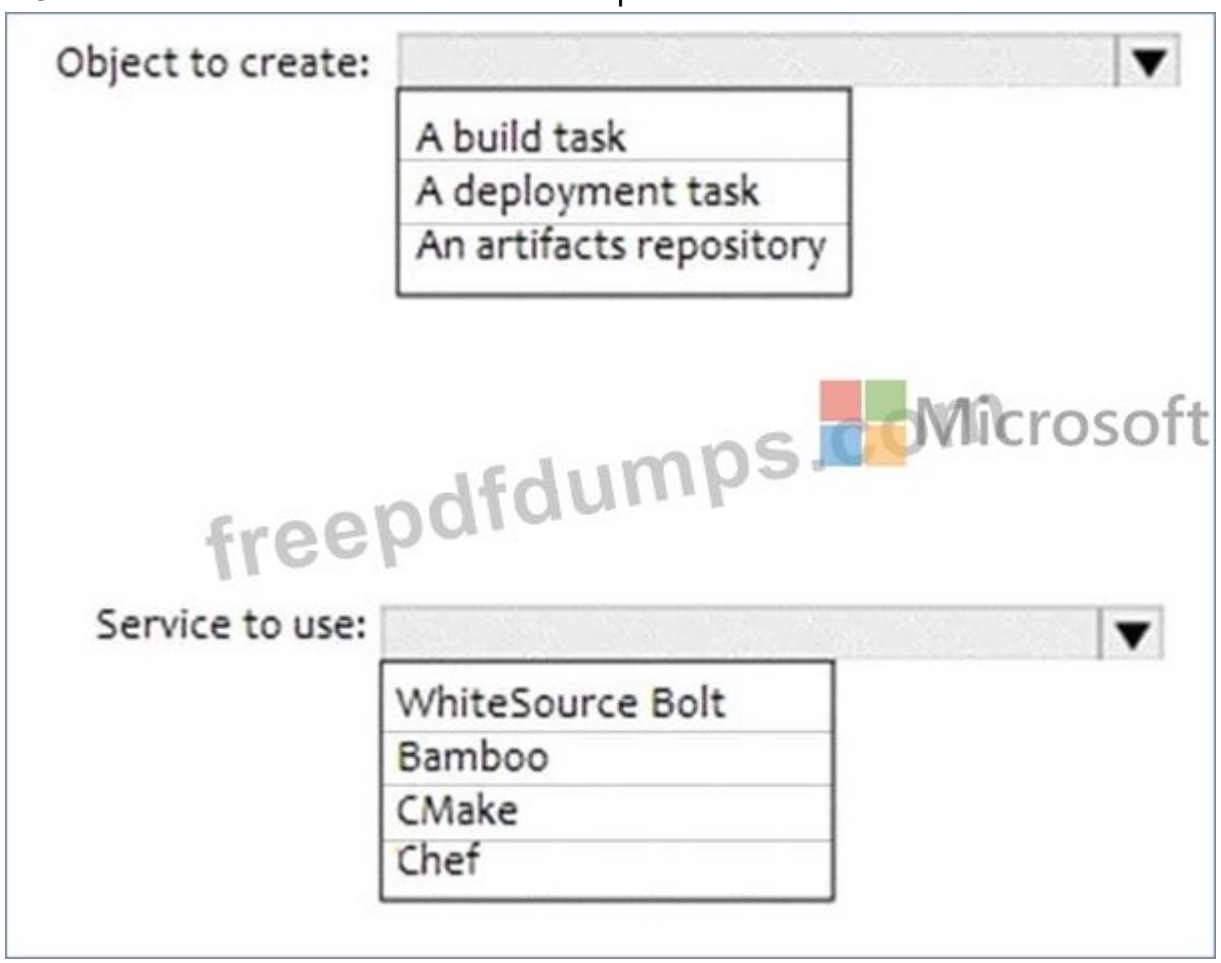
Scenario: By default, all releases must remain available for 30 days, except for production releases, which must be kept for 60 days.
Box 1: Set the default retention policy to 30 days
The Global default retention policy sets the default retention values for all the build pipelines. Authors of build pipelines can override these values.
Box 2: Set the stage retention policy to 60 days
You may want to retain more releases that have been deployed to specific stages.
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/policies/retention

NEW QUESTION: 70
You have 50 Node.js-based projects that you scan by using WhiteSource. Each project includes Package.json, Package-lock.json, and Npm-shrinkwrap.json files.
You need to minimize the number of libraries reports by WhiteSource to only the libraries that you explicitly reference.
What should you do?
A. Configure the File System Agent plug in.
B. Delete Package lock.json.
C. Configure the Artifactory plug-in.
D. Add a devDependencies section to Package-lock.json.
Answer: D (LEAVE A REPLY)
Separate Your Dependencies
Within your package.json file be sure you split out your npm dependencies between devDependencies and (production) dependencies. The key part is that you must then make use of the --production flag when installing the npm packages. The --production flag will exclude all packages defined in the devDependencies section.
References:
https://blogs.msdn.microsoft.com/visualstudioalmrangers/2017/06/08/manage-your-open-source-usage-and-security-as-reported-by-your-cicd-pipeline/

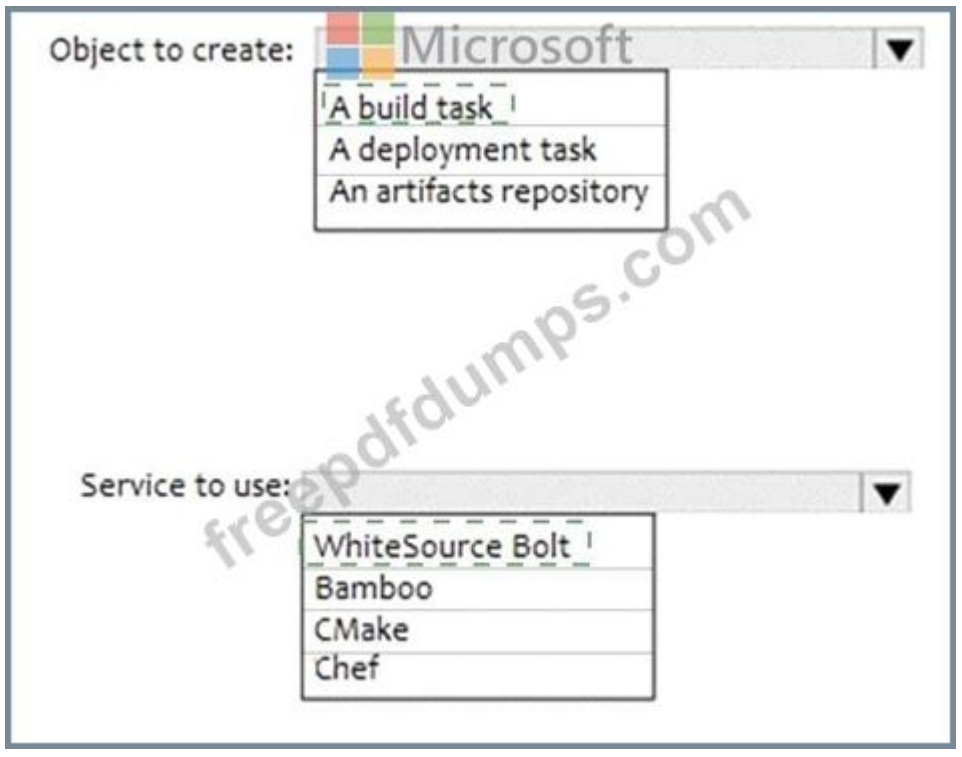
NEW QUESTION: 71
Your company uses the following resources:
* Windows Server 2019 container images hosted in an Azure Container Registry.
* Azure virtual machines that run the latest version of Ubuntu
* An Azure Log Analytics workspace
* Azure Active Directory (Azure AD)
* An Azure key vault
For which 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: B,C (LEAVE A REPLY)
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

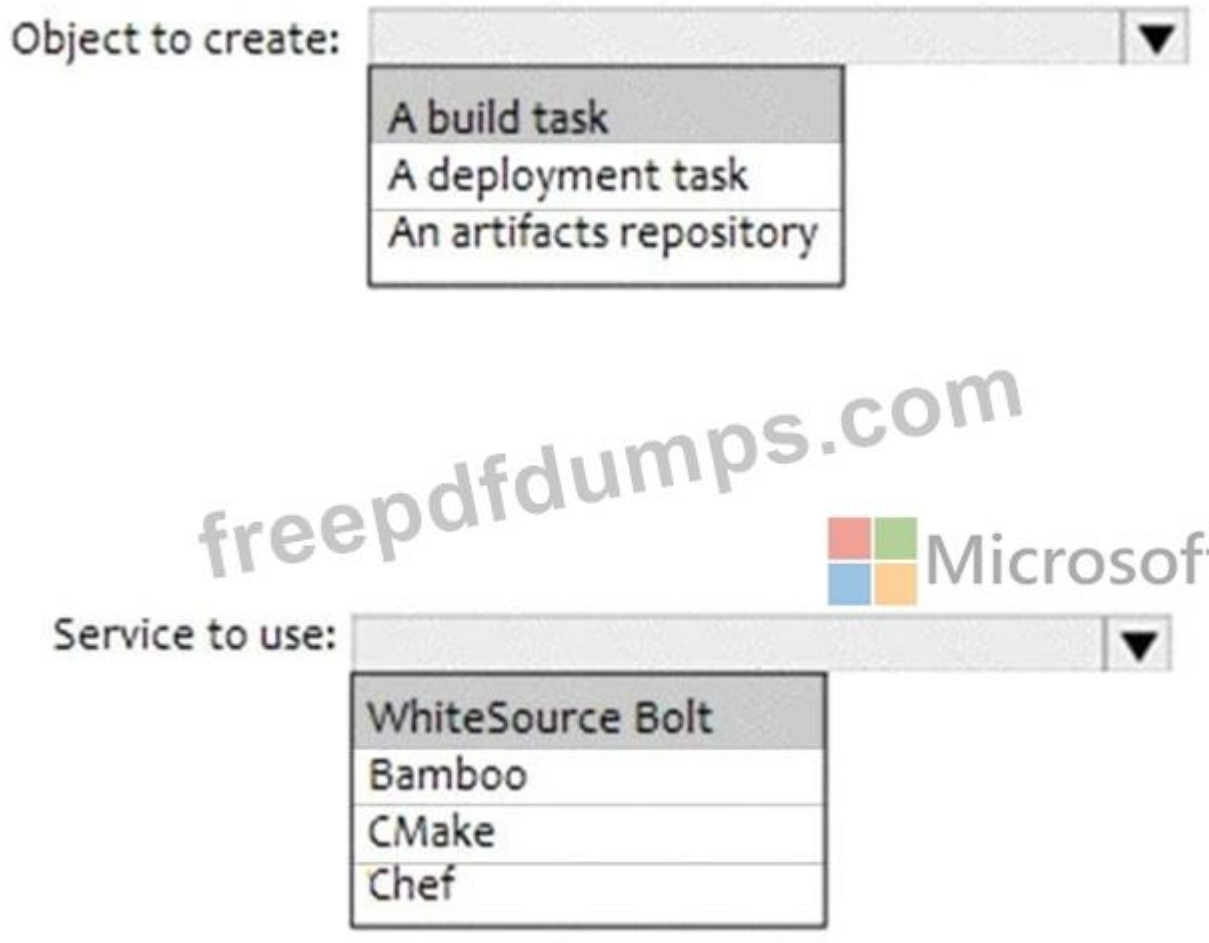
NEW QUESTION: 72
You have an Azure DevOps project that contains a build pipeline. The build pipeline uses approximately 50 open source libraries.
You need to ensure that the project can be scanned for known security vulnerabilities in the open source libraries.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation



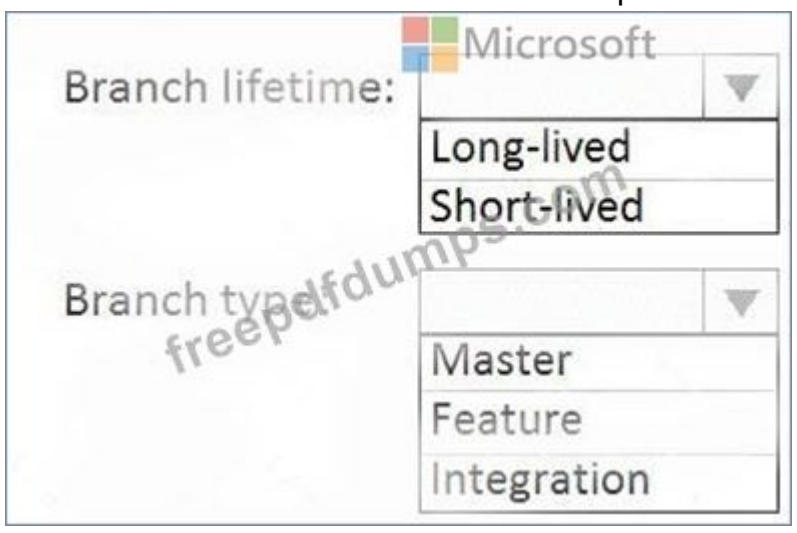
Box 1: A Build task

Trigger a build

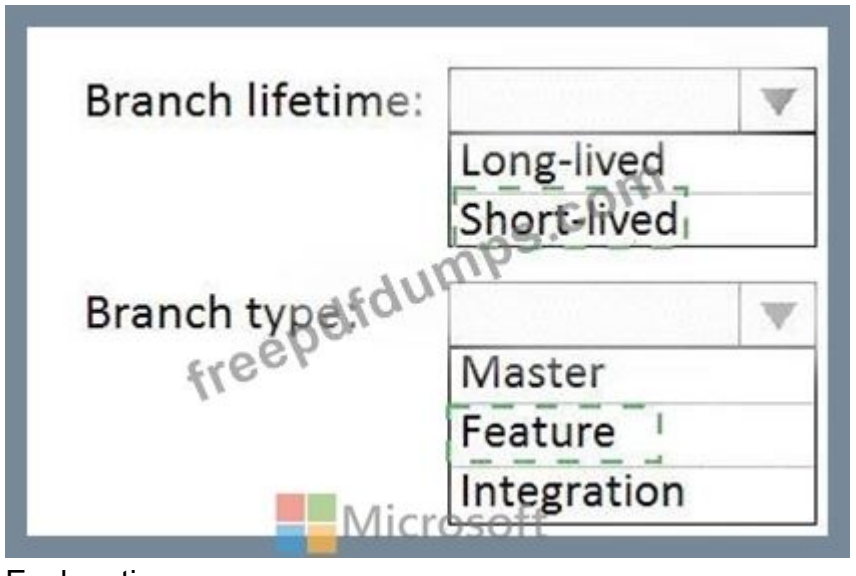
You have a Java code provisioned by the Azure DevOps demo generator. You will use WhiteSource Bolt extension to check the vulnerable components present in this code.

* Go to Builds section under Pipelines tab, select the build definition WhiteSourceBolt and click on Queue to trigger a build.
* To view the build in progress status, click on ellipsis and select View build results.
Box 2: WhiteSource Bolt
WhiteSource is the leader in continuous open source software security and compliance management.
WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated denitive database of open source repositories.
References:
https://www.azuredevopslabs.com/labs/vstsextend/whitesource/

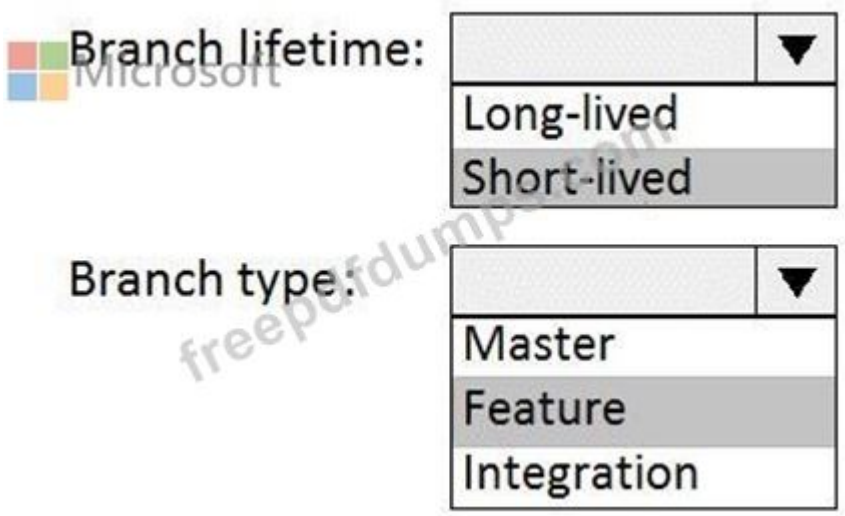
NEW QUESTION: 73
Your company uses Git as a source code control system for a complex app named App1.
You plan to add a new functionality to App1.
You need to design a branching model for the new functionality.
Which branch lifetime and branch time should you use in the branching model? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation

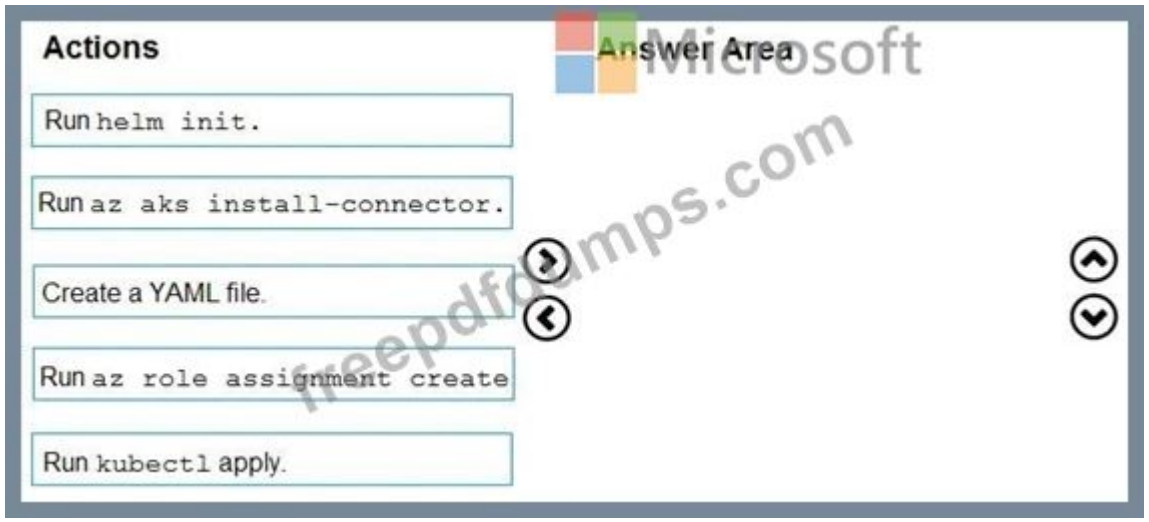


Branch lifetime: Short-lived
Branch type: Feature
Feature branches are used when developing a new feature or enhancement which has the potential of a development lifespan longer than a single deployment. When starting development, the deployment in which this feature will be released may not be known.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

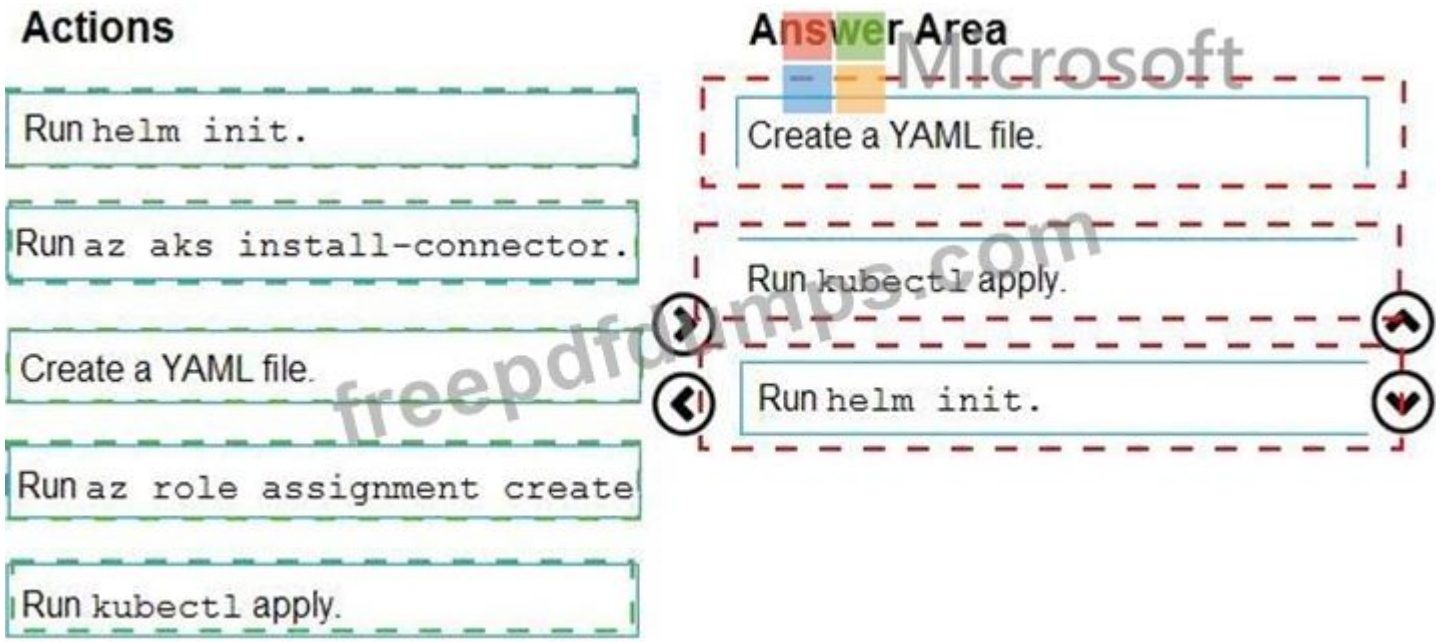
NEW QUESTION: 74
Note: This question is part of a ser les of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question m this section, you will NOT be able to return to it As a result, these questions will not appear m the review screen
You integrate a cloud-hosted Jenkins server and a new Azure Dev Ops deployment.
You need Azure Dev Ops lo send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.
Solution: You create an email subscription to an Azure DevOps notification.
Does this meet the goal?
A. Yes
B. NO
Answer: B (LEAVE A REPLY)
Explanation
You can create a service hook for Azure DevOps Services and TFS with Jenkins.
References:
https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins

NEW QUESTION: 75
You have an Azure Kubermets Service (AKS) implementation that is RBAC-enabled You plan to use Azure Container Instances as a hosted development environment to run containers in the AKS implementation.
You need to conjure Azure Container Instances as a hosted environment for running me containers in AKS.
Which three actions should you perform m sequence?

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



Answer:



Explanation

Step 1: Create a YAML file.

If your AKS cluster is RBAC-enabled, you must create a service account and role binding for use with Tiller.

To create a service account and role binding, create a file named rbac-virtual-kubelet.yaml Step 2: Run kubectl apply.

Apply the service account and binding with kubectl apply and specify your rbac-virtual-kubelet.yaml file.

Step 3: Run helm init.

Configure Helm to use the tiller service account:

helm init --service-account tiller

You can now continue to installing the Virtual Kubelet into your AKS cluster.

References: https://docs.microsoft.com/en-us/azure/aks/virtual-kubelet

NEW QUESTION: 76

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

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

Answer:

See solution below.

Explanation

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

* Sign in to Azure portal
* Locate virtual machine VM1.
* Select Identity
* Enable the system-assigned identity for VM1 by setting the Status to On.

Note: Enabling a system-assigned managed identity is a one-click experience. You can either enable it during the creation of a VM or in the properties of an existing VM.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm

NEW QUESTION: 77

You have an Azure DevOps organization named Contoso.

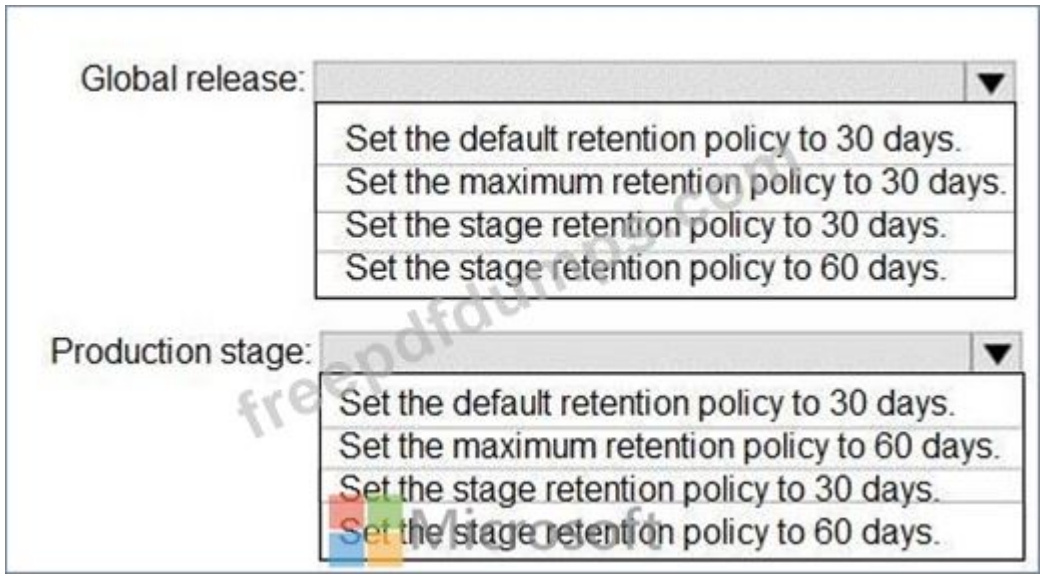
You need to recommend an authentication mechanism that meets the following requirements:

* Supports authentication from Git
* Minimizes the need to provide credentials during authentication

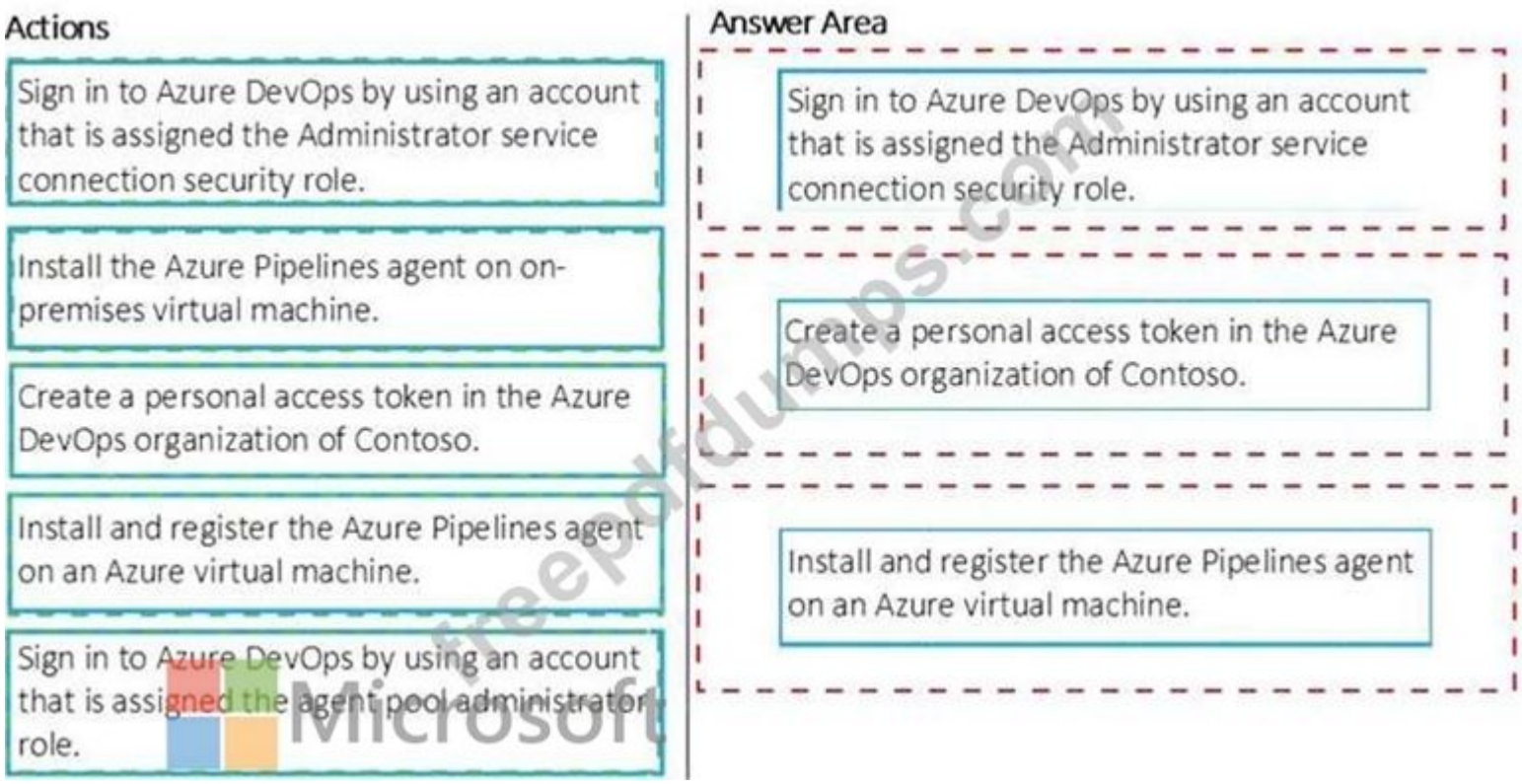
What should you recommend?

A. personal access tokens (PATs) in Azure DevOps
B. user accounts in Azure Active Directory (Azure AD)
C. managed identities in Azure Active Directory (Azure AD)
D. Alternate credentials in Azure DevOps
Answer: A (LEAVE A REPLY)

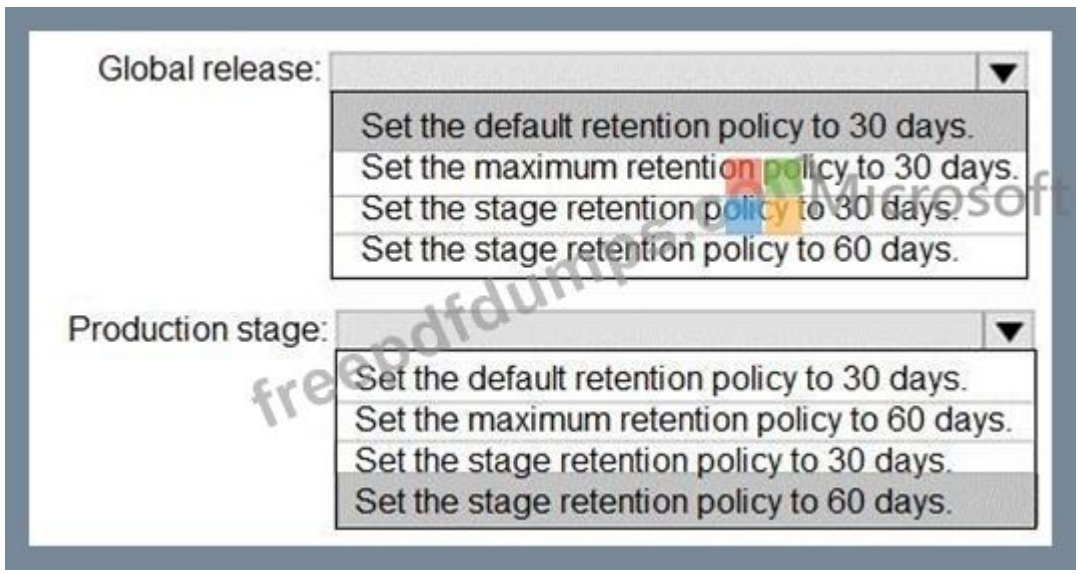
NEW QUESTION: 78
How should you configure the release retention policy for the investment planning applications suite? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation



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

Box 1: Set the default retention policy to 30 days

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

Box 2: Set the stage retention policy to 60 days

You may want to retain more releases that have been deployed to specific stages.

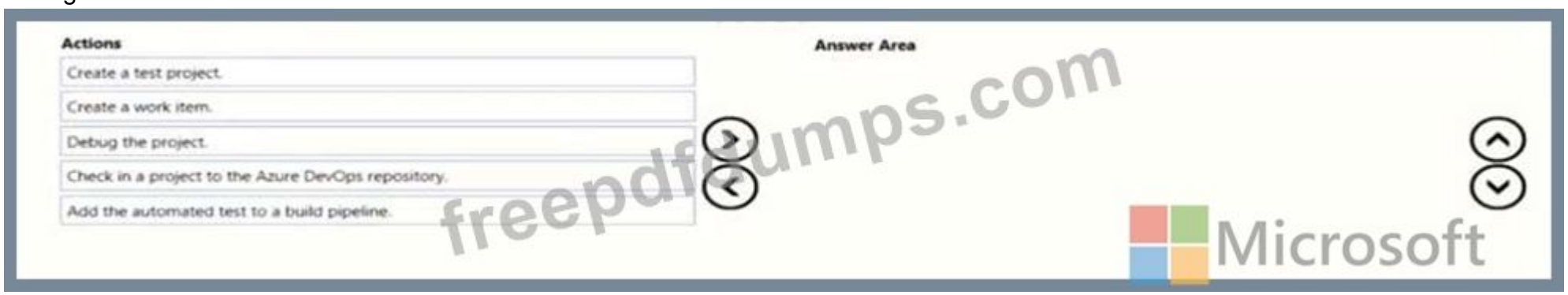
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/policies/retention

NEW QUESTION: 79

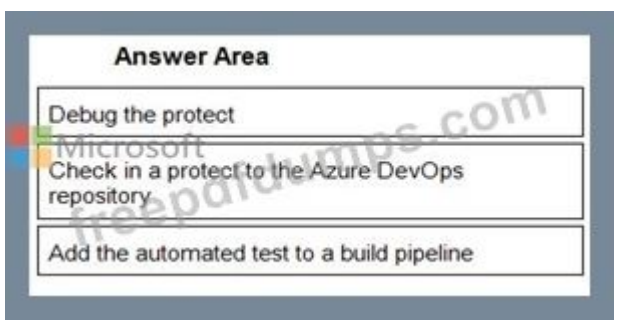
You have a protect in Azure DevOps.

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.



Answer:

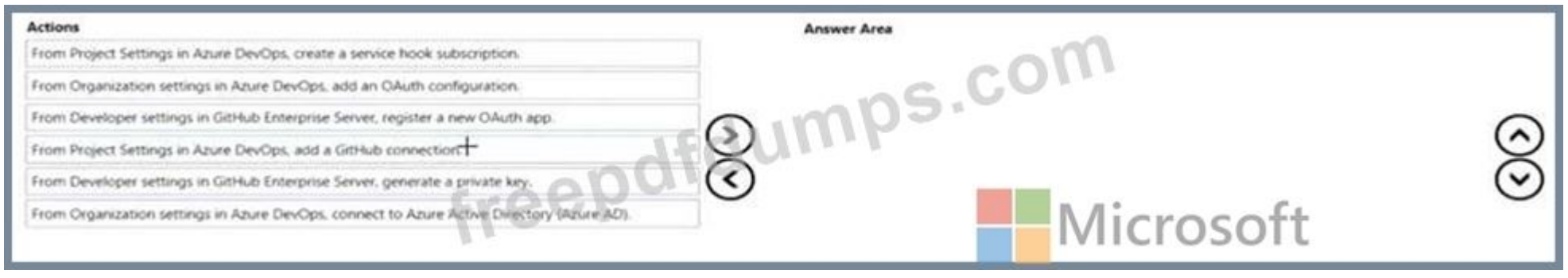


1 - Debug the protect
2 - Check in a protect to the Azure DevOps repository
3 - Add the automated test to a build pipeline

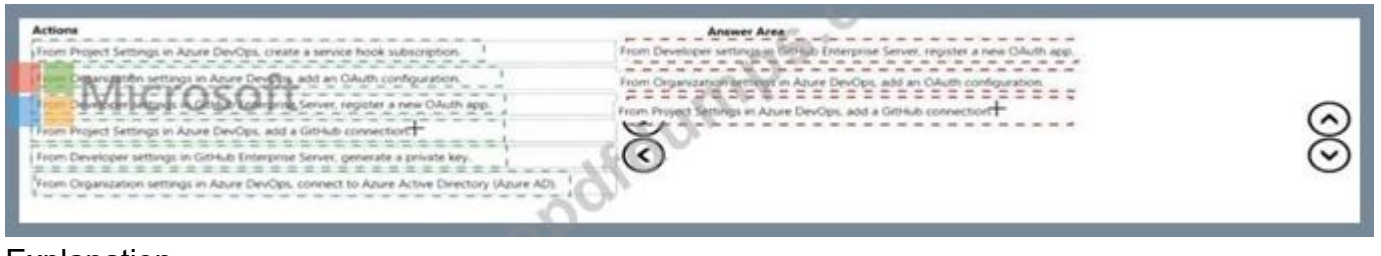
Explanation:
The process to associate an automated test with a test case is:
* Create a test project containing your automated test. What types of tests are supported?
* Check your test project into an Azure DevOps or Team Foundation Server (TFS) repository.
* Create a build pipeline for your project, ensuring that it contains the automated test. What are the differences if I am still using a XAML build?
* 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

NEW QUESTION: 80
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 (LEAVE A REPLY)
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

NEW QUESTION: 81
You use GitHub Enterprise Server as a source code repository.
You create an Azure DevOps organization named Contoso.
In the Contoso organization, you create a project named Project 1.
You need to link GitHub commits, pull requests, and issues to the work items of Project 1. The solution must use OAuth-based authentication
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation

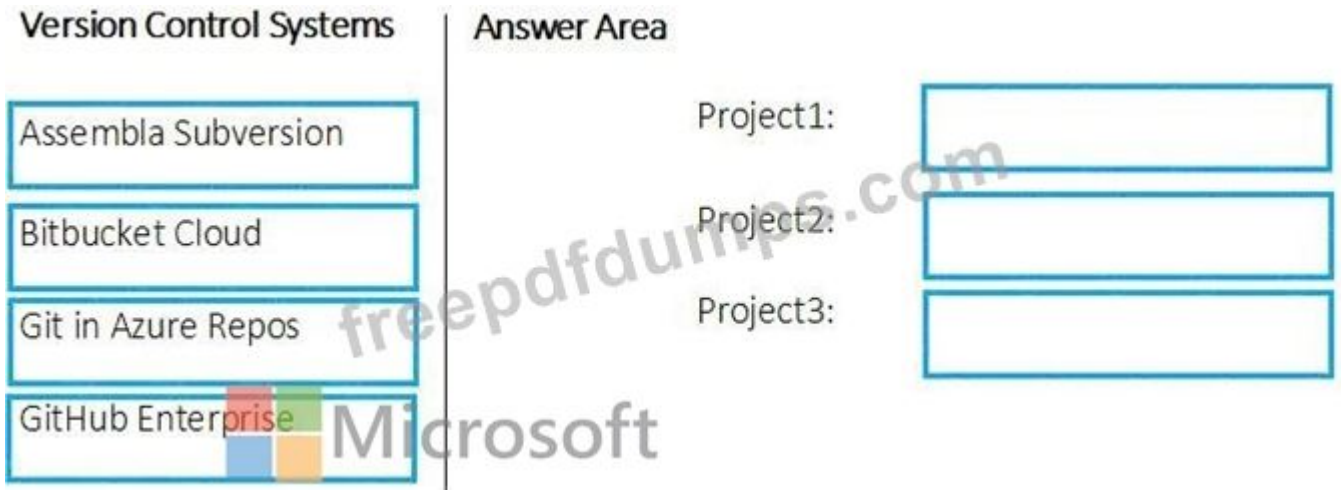
Step 1: From Developer settings in GitHub Enterprise Server, register a new OAuth app.
If you plan to use OAuth to connect Azure DevOps Services or Azure DevOps Server with your GitHub Enterprise Server, you first need to register the application as an OAuth App Step 2: Organization settings in Azure DevOps, add an OAuth configuration Register your OAuth configuration in Azure DevOps Services.
Note:
* Sign into the web portal for Azure DevOps Services.
* Add the GitHub Enterprise Oauth configuration to your organization.
* Open Organization settings>Oauth configurations, and choose Add Oauth configuration.
* Fill in the form that appears, and then choose Create.
Step 3: From Project Settings in Azure DevOps, add a GitHub connection.
Connect Azure DevOps Services to GitHub Enterprise Server
Choose the Azure DevOps logo to open Projects, and then choose the Azure Boards project you want to configure to connect to your GitHub Enterprise repositories.
Choose (1) Project Settings, choose (2) GitHub connections and then (3) Click here to connect to your GitHub Enterprise organization.
Reference:
https://docs.microsoft.com/en-us/azure/devops/boards/github/connect-to-github

NEW QUESTION: 82
You are configuring Azure Pipelines for three projects in Azure DevOps as shown in the following table.

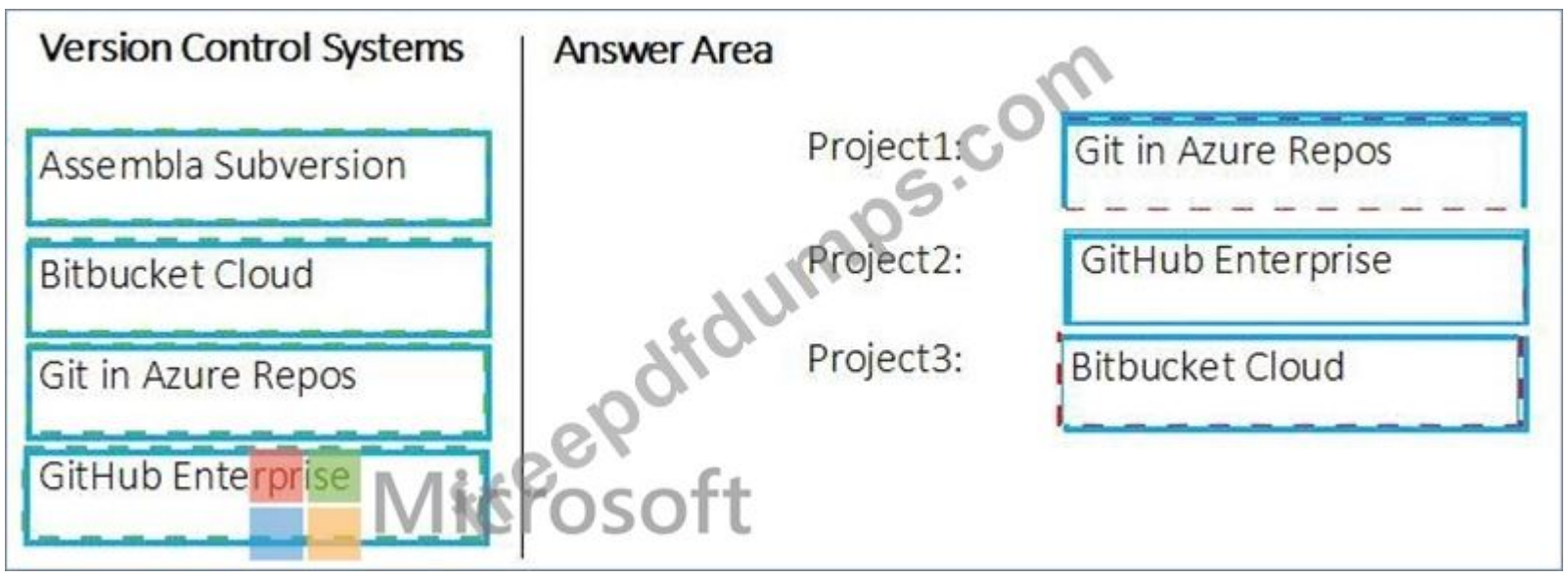
Project name	Project Details
Project1	The project team provides preconfigured YAML files that it wants to use to manage future pipeline configuration changes.
Project2	The sensitivity of the project requires that the source code be hosted on the managed Windows server on your company's network.
Project3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



Answer:



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.

NEW QUESTION: 83
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 (LEAVE A REPLY)
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

NEW QUESTION: 84
You add the virtual machines as managed nodes in Azure Automation State Configuration.
You need to configure the computer in Group7.

What should you do?

A. Run the Register-AzureRmAutomationDscNode Azure Powershell cmdlet.

B. Modify the ConfigurationMode property of the Local Configuration Manager (LCM).

C. Install PowerShell Core.

D. Modify the RefreshMode property of the Local Configuration Manager (LCM).

Answer: A (LEAVE A REPLY)

Topic 1, Case Study: 2Overview

Existing Environment

This is a case study Case studies are not limed separately. You can use as much exam time at you would like to complete each case. However there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided m the case study Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of the case study, a review screen will appear. This screen allows you to review your answers and to mate changes before you move to the next section of the exam, After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment and problem statements. If the case study has an All Information tab, note that the information displayed on identical to the Information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Requirements

Contoso plans to improve its IT development and operations processes implementing Azue DevOps principles.

Contoso has an Azure subscription and creates an Azure DevOPs organization.

The Azure DevOps organization includes:

The Docker extension

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

The Azure subscription contains an Azure Automation account.

Planned Changes

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

Project name	Project details
Project1	Project1 will provide support for incremental builds and third-party SDK components.
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.
Project3	Project3 will be integrated with SonarQube.
Project4	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.
Project5	Project5 will contain a Git repository in Azure Repos and a continuous integration trigger that will initiate a build in response to any change except for changes within /folder1 of the repository.
Project6	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.
Project7	Project7 will contain a target deployment group named Group7 that maps to Pool7. Project7 will use Azure Automation State Configuration to maintain the desired state of the computers in Group7.

Technical Requirements

Contoso identities the following technical requirements:

* Implement build agents rot Project 1.
* Whenever possible, use Azure resources
*Avoid using deprecated technologies
* Implement a code flow strategy for Project2 that will:
*Enable Team 2 to submit pull requests for Project2.
* Enable Team 2 to work independently on changes to a copy of Project?
* Ensure that any intermediary changes performed by Tram2 on a copy of Project2 will be subject to the same restrictions as the ones defied in the build policy of Project2.
* Whenever possible. Implement automation and minimize administrative effort.
* Implement Protect3, Project5, Project6, and Project7 based on the planned changes.
* Implement Project4 and configure the project to push Docker images to Azure Container Reentry.

NEW QUESTION: 85

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

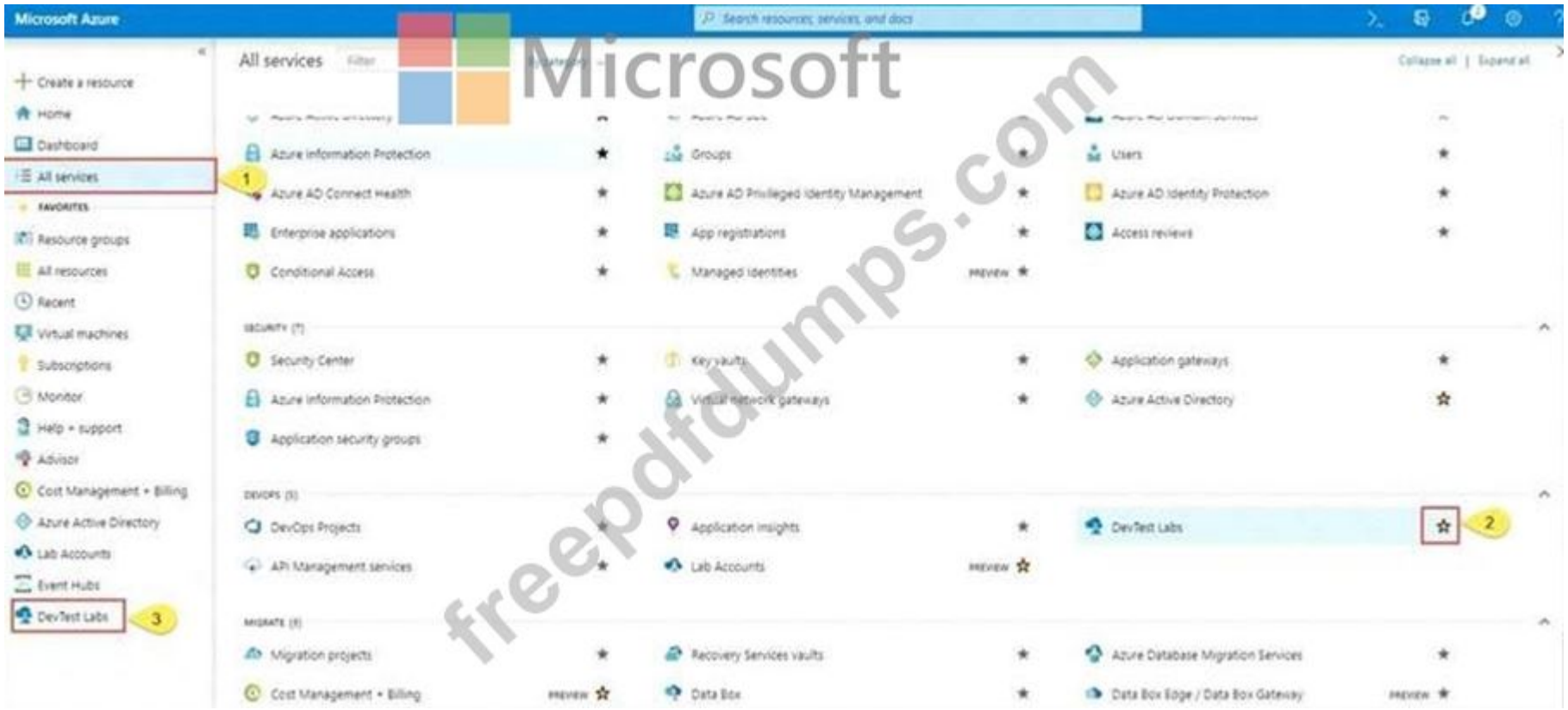
You plan to create a release pipeline that will deploy Azure resources by using Azure Resource Manager templates. The release pipeline will create the following resources:

* Two resource groups
* Four Azure virtual machines in one resource group

* Two Azure SQL databases in other resource group
You need to recommend a solution to deploy the resources.
Solution: Create two standalone templates, each of which will deploy the resources in its respective group.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Explanation
Use a main template and two linked templates.
References: https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-linked-templates

NEW QUESTION: 86
Your company is building a mobile app that targets Android devices and OS devices. Your team uses Azure DevOps to manage all work items and release cycles. You need to recommend a solution to perform the following tasks
* Collect crash reports for issue analysis
* Distribute beta releases to your testers.
* Get user feedback on the functionality of new apps.
What should you include in the recommendation?
A. Microsoft Visual Studio App Center integration
B. the Microsoft Test & Feedback extension
C. Jenkins integration
D. Azure Application Insights widgets
Answer: A (LEAVE A REPLY)

NEW QUESTION: 87
You need to create a virtual machine template in an Azure DevTest Labs environment named az400-9940427-dtl1. The template must be based on Windows Server 2016 Datacenter. Virtual machines created from the template must include the selenium tool and the Google Chrome browser.
To complete this task, sign in to the Microsoft Azure portal.
Answer:
See solution below.
Explanation
1. Open Microsoft Azure Portal
2. Select All Services, and then select DevTest Labs in the DEVOPS section.



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

References:

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

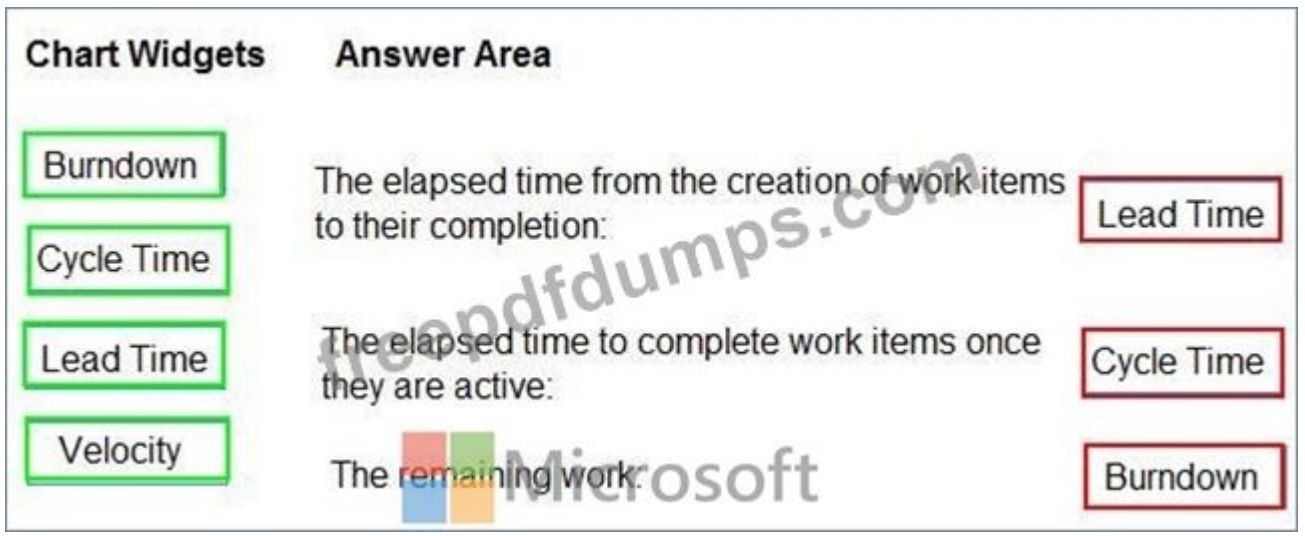
NEW QUESTION: 88

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

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

NOTE: Each correct selection is worth one point.

Answer:



Explanation:

Box 1: Lead time

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

Box 2: Cycle time

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

Box 3: Burndown

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

Incorrect Answers:

References:

https://docs.microsoft.com/en-us/azure/devops/report/dashboards/velocity-guidance?view=vsts

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

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

NEW QUESTION: 89

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 Dependency agent
B. the Azure Network Watcher Agent for Windows
C. the Telegraf agent
D. the Azure Log Analytics agent
Answer: (SHOW ANSWER)
Explanation
The following table provide a quick comparison of the Azure Monitor agents for Windows.

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

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

NEW QUESTION: 90
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

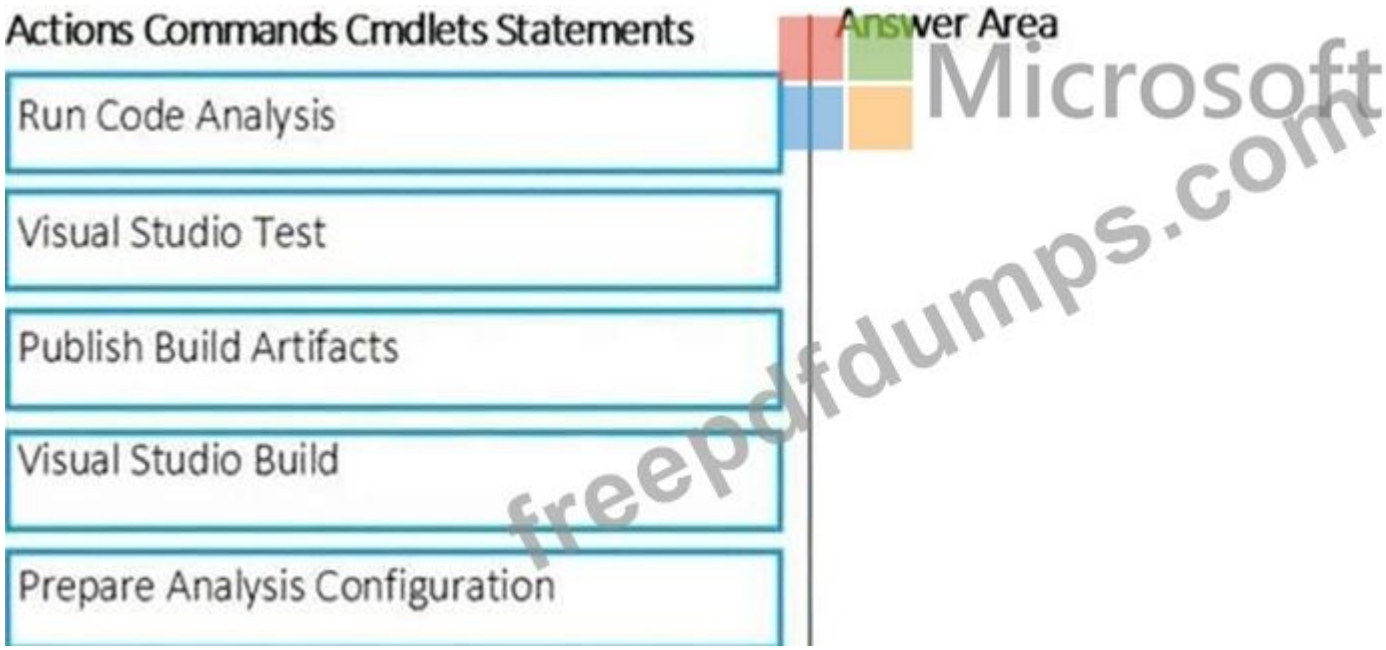
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You plan to update the Azure DevOps strategy of your company.
You need to identify the following issues as they occur during the company's development process:
* Licensing violations
* Prohibited libraries
Solution: You implement continuous integration.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
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/

NEW QUESTION: 91
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 (LEAVE A REPLY)
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

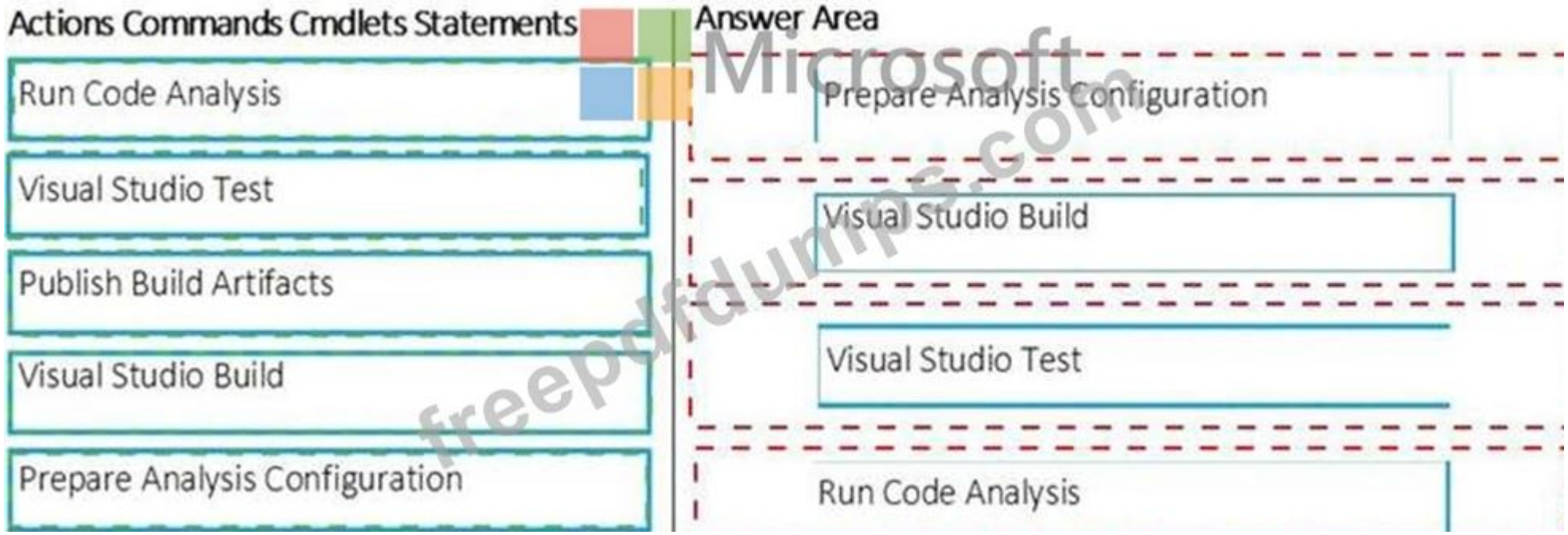
NEW QUESTION: 92

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

NEW QUESTION: 93
DRAG DROP
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.



Answer:



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

NEW QUESTION: 94
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 (DSQ 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.

Answer:

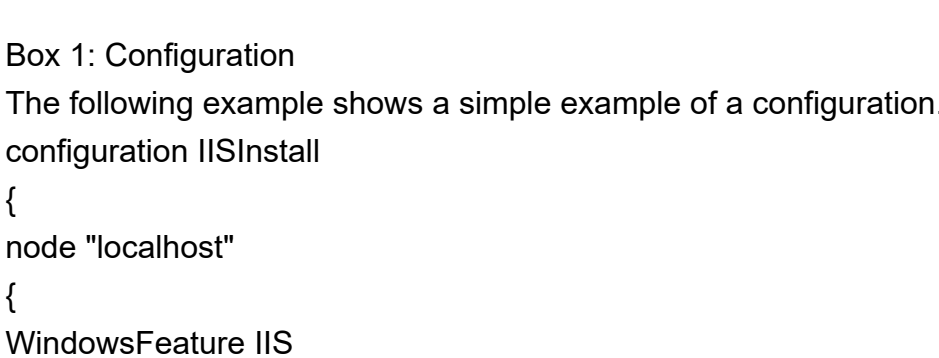
Explanation

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

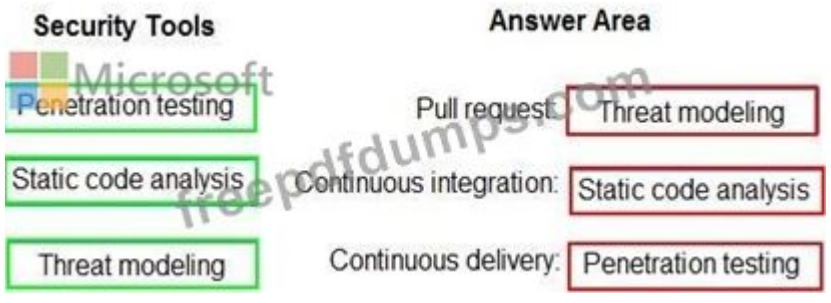
```
configuration IISInstall
{
node "localhost"
{
WindowsFeature IIS
{
Ensure = "Present"
Name = "Web-Server"
}
}
}
```

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

NEW QUESTION: 95
You need to increase the security of your team's development process.
Which type of security tool should you recommend for each stage of the development process? To answer, drag the appropriate security toots to the correct stages. Each security tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content
NOTE: Each correct selection is worth one point.



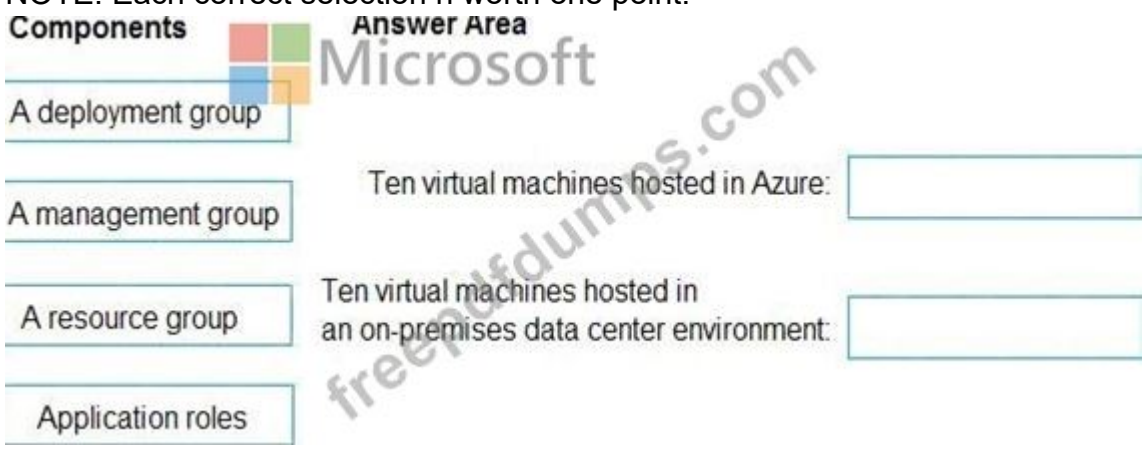
Answer:



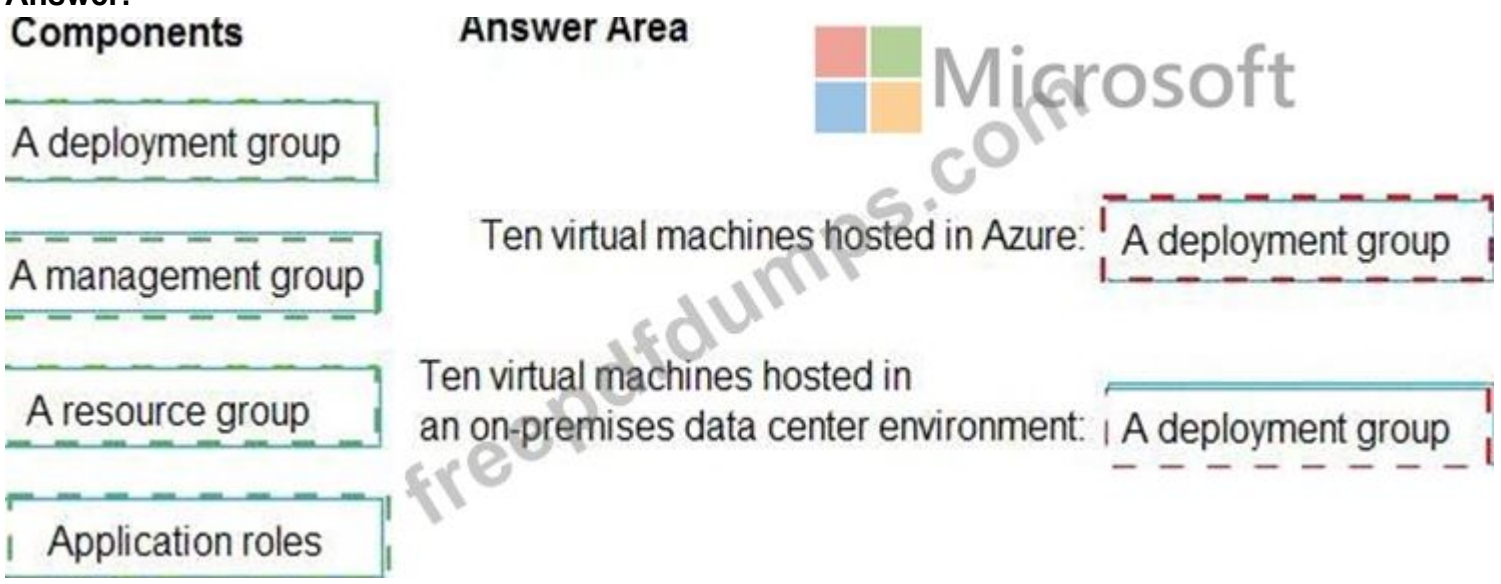
Explanation:
https://docs.microsoft.com/en-us/azure/devops/migrate/security-validation-cicd-pipeline?view=azure-devops&viewFallbackFrom=vsts
So:
PR: Static Code Analysis

CI: Static Code Analysis
CD: PenTest

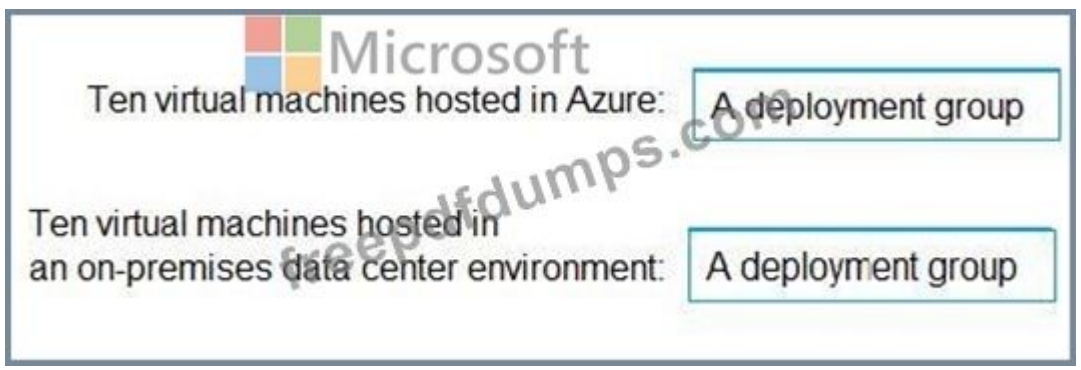
NEW QUESTION: 96
Your company plans to deploy an application to the following endpoints:
* Ten virtual machines hosted in Azure.
* Ten virtual machines hosted in an on-premises data center environment All the virtual machines have the- Azure Pipelines agent.
You need to implement a release strategy for deploying the application to the endpoints.
What should you recommend using to deploy the application to the endpoints? To answer, drag the appropriate components to the correct endpoint.
Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or soon to view content
NOTE: Each correct selection n worth one point.



Answer:



Explanation



Box 1: A deployment group

When authoring an Azure Pipelines or TFS Release pipeline, you can specify the deployment targets for a job using a deployment group.

If the target machines are Azure VMs, you can quickly and easily prepare them by installing the Azure Pipelines Agent Azure VM extension on each of the VMs, or by using the Azure Resource Group Deployment task in your release pipeline to create a deployment group dynamically.

Box 2: A deployment group

References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deployment-groups

NEW QUESTION: 97

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

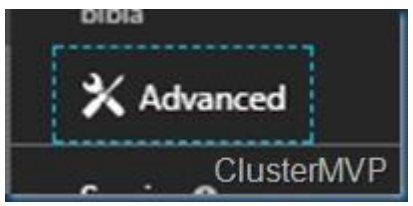
To complete this task, sign in to the Microsoft Azure portal.

A. 1. Open Microsoft Azure Portal and Log into your Azure account.

2. Select network security group (NSG) named az400-9940427-nsg1

3. Select Settings, Outbound security rules, and click Add

4. Click Advanced



5. Change the following settings:

* Destination Port range: 8080

* Protocol. TCP

* Action: Allow

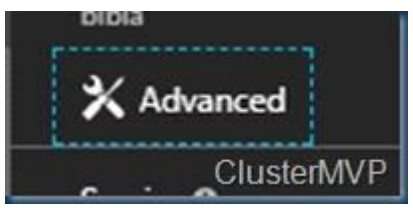
Note: By default, Azure DevOps Server uses TCP Port 8080.

B. 1. Open Microsoft Azure Portal and Log into your Azure account.

2. Select network security group (NSG) named az400-9940427-nsg1

3. Select Settings, Outbound security rules, and click Add

4. Click Advanced



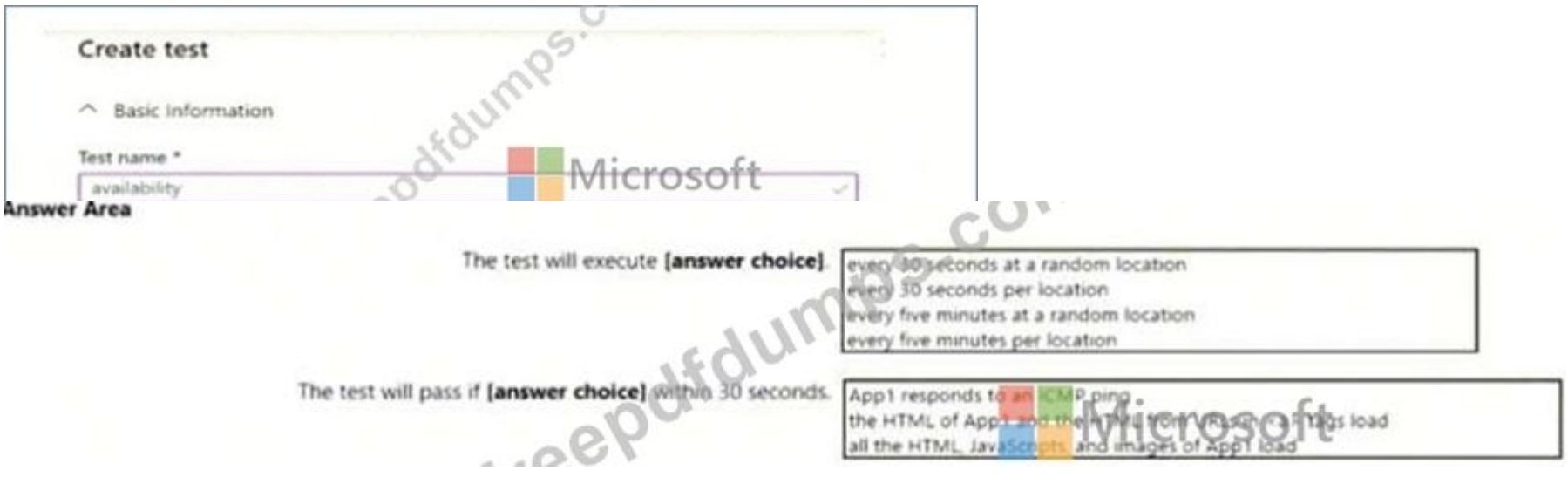
5. Change the following settings:

* Destination Port range: 8080

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

NEW QUESTION: 98
You manage an Azure web app that supports an e-commerce website.
You need to increase the logging level when the web app exceeds normal usage patterns. The solution must minimize administrative overhead.
Which two resources should you include in the solution? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. an Azure Automation runbook
B. an Azure Monitor alert that has a dynamic threshold
C. an Azure Monitor alert that has a static threshold
D. the Azure Monitor autoscale settings
E. an Azure Monitor alert that uses an action group that has an email action
Answer: A,B (LEAVE A REPLY)
B: Metric Alert with Dynamic Thresholds detection leverages advanced machine learning (ML) to learn metrics' historical behavior, identify patterns and anomalies that indicate possible service issues. It provides support of both a simple UI and operations at scale by allowing users to configure alert rules through the Azure Resource Manager API, in a fully automated manner.
A: You can use Azure Monitor to monitor base-level metrics and logs for most services in Azure. You can call Azure Automation runbooks by using action groups or by using classic alerts to automate tasks based on alerts.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-dynamic-thresholds
https://docs.microsoft.com/en-us/azure/automation/automation-create-alert-triggered-runbook

NEW QUESTION: 99
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.



Answer:

Answer Area

The test will execute **[answer choice]** every 30 seconds at a random location / every 30 seconds per location / every five minutes at a random location / every five minutes per location

The test will pass if **[answer choice]** within 30 seconds. App1 responds to an ICMP ping / the HTML of App1 and the HTML from URLs in <a> tags load / all the HTML, JavaScripts, and images of App1 load

Explanation

Answer Area

The test will execute **[answer choice]** every five minutes per location

The test will pass if **[answer choice]** within 30 seconds. App1 responds to an ICMP ping

NEW QUESTION: 100

You are implementing an Azure DevOps strategy for mobile devices using App Center.

You plan to use distribution groups to control access to releases.

You need to create the distribution groups shown in the following table.

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

Which type of distribution group should you use for each group? To answer, drag the appropriate group types to the correct locations. Each group type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Answer Area

Private

Public

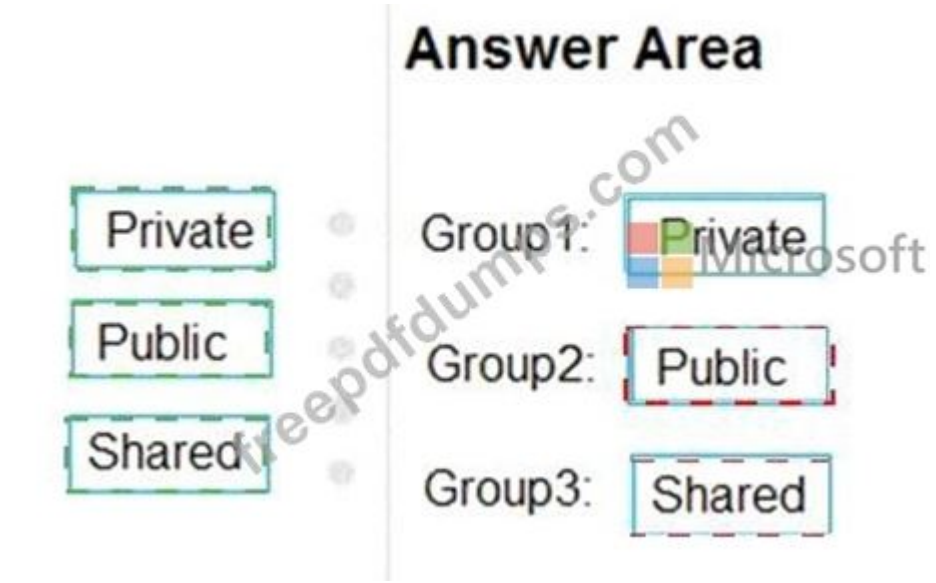
Shared

Group1:

Group2:

Group3:

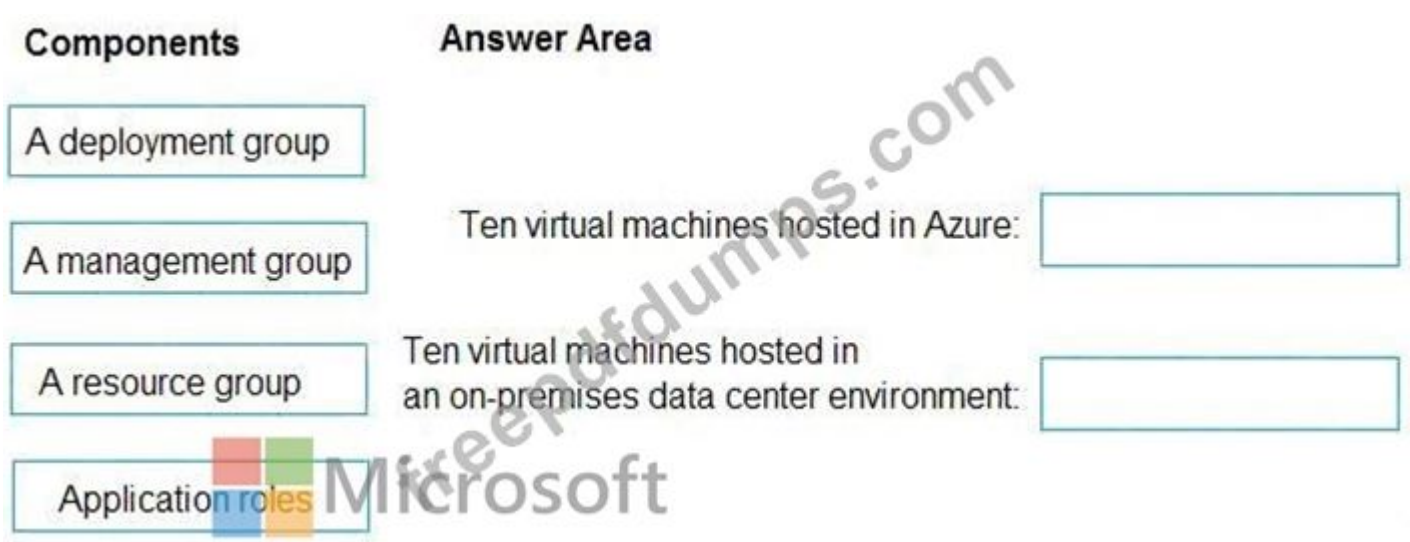
Answer:



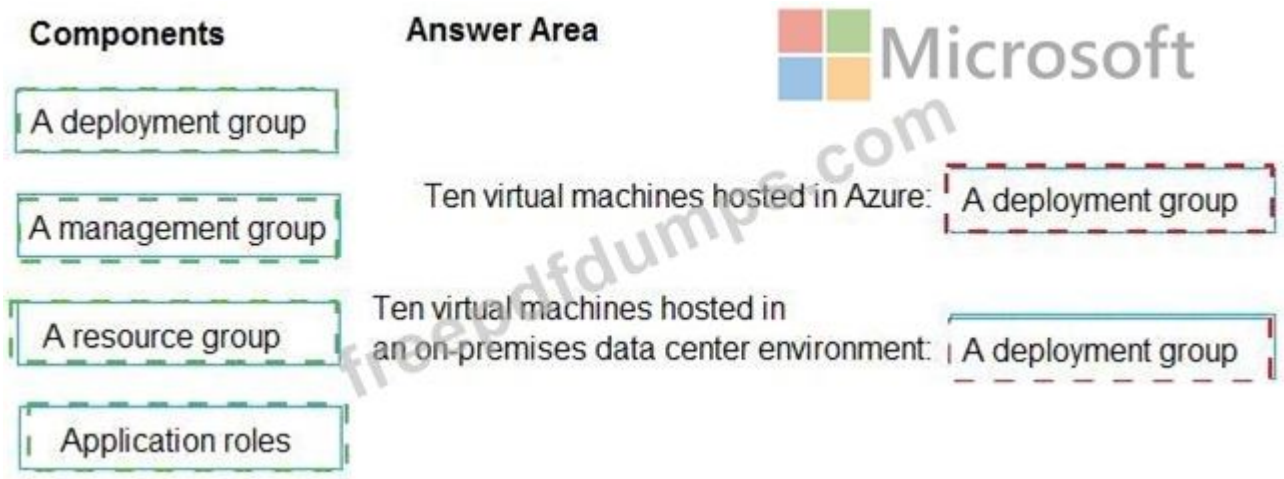
Explanation

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

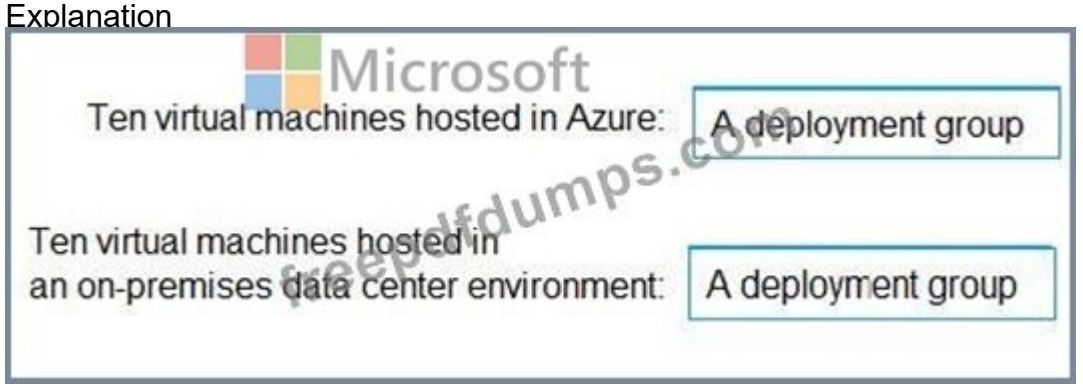
NEW QUESTION: 101
Your company plans to deploy an application to the following endpoints:
* Ten virtual machines hosted in Azure.
* Ten virtual machines hosted in an on-premises data center environment All the virtual machines have the- Azure Pipelines agent.
You need to implement a release strategy for deploying the application to the endpoints.
What should you recommend using to deploy the application to the endpoints? To answer, drag the appropriate components to the correct endpoint.
Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or soon to view content
NOTE: Each correct selection n worth one point.



Answer:



Explanation



Box 1: A deployment group

When authoring an Azure Pipelines or TFS Release pipeline, you can specify the deployment targets for a job using a deployment group.

If the target machines are Azure VMs, you can quickly and easily prepare them by installing the Azure Pipelines Agent Azure VM extension on each of the VMs, or by using the Azure Resource Group Deployment task in your release pipeline to create a deployment group dynamically.

Box 2: A deployment group

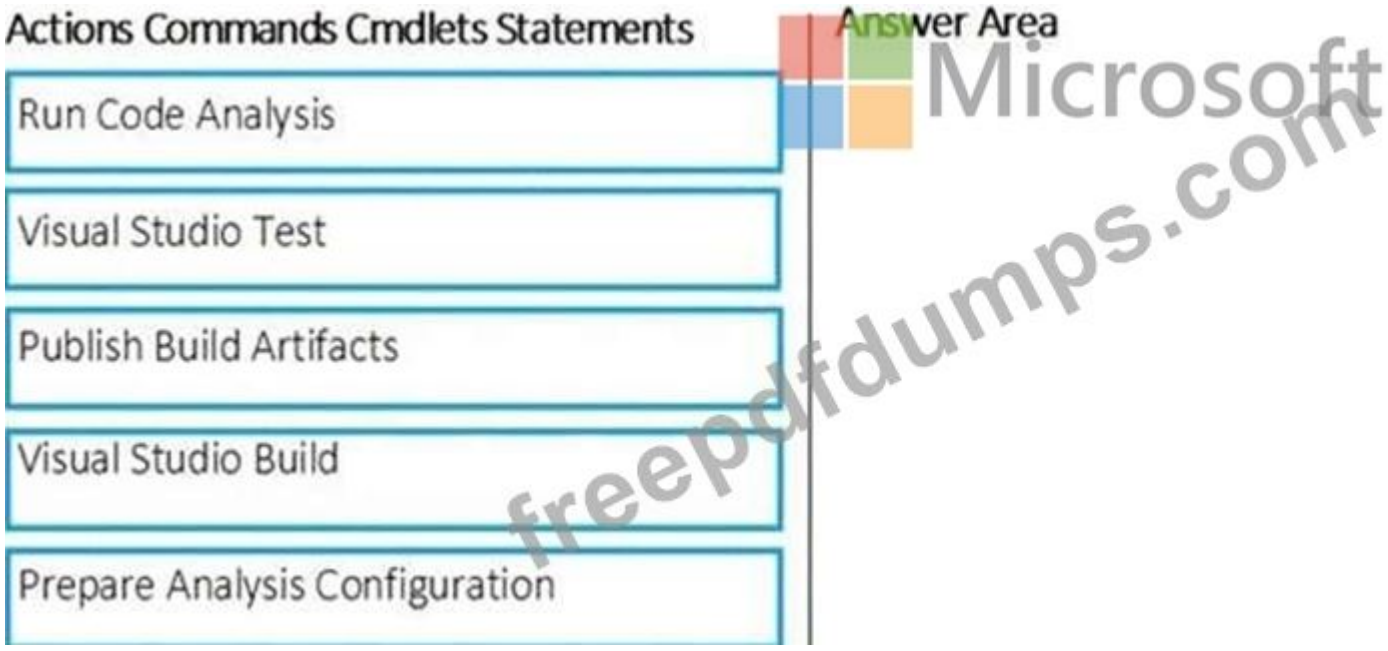
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deployment-groups

NEW QUESTION: 102

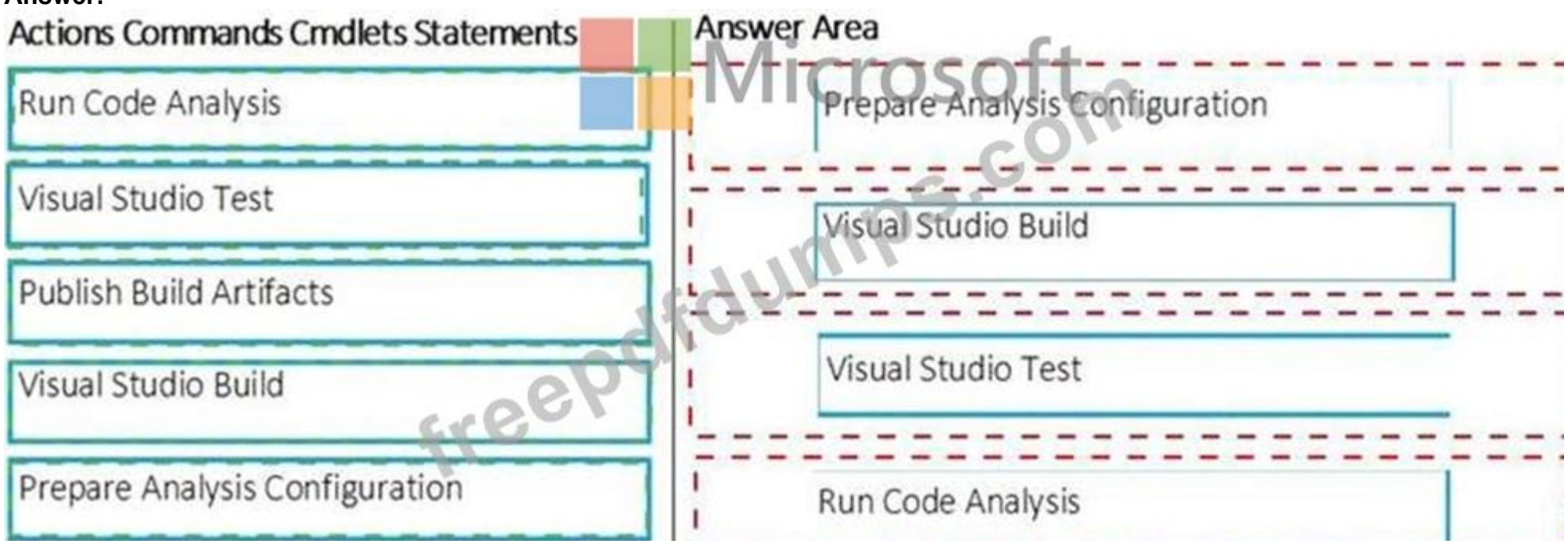
You are developing a full Microsoft .NET Framework solution that includes unit tests.

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.



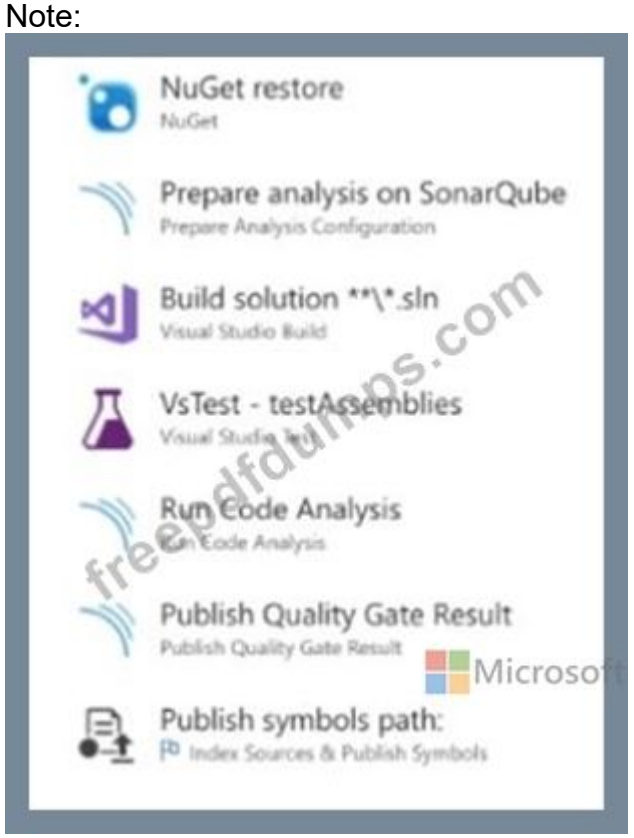
Answer:



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:



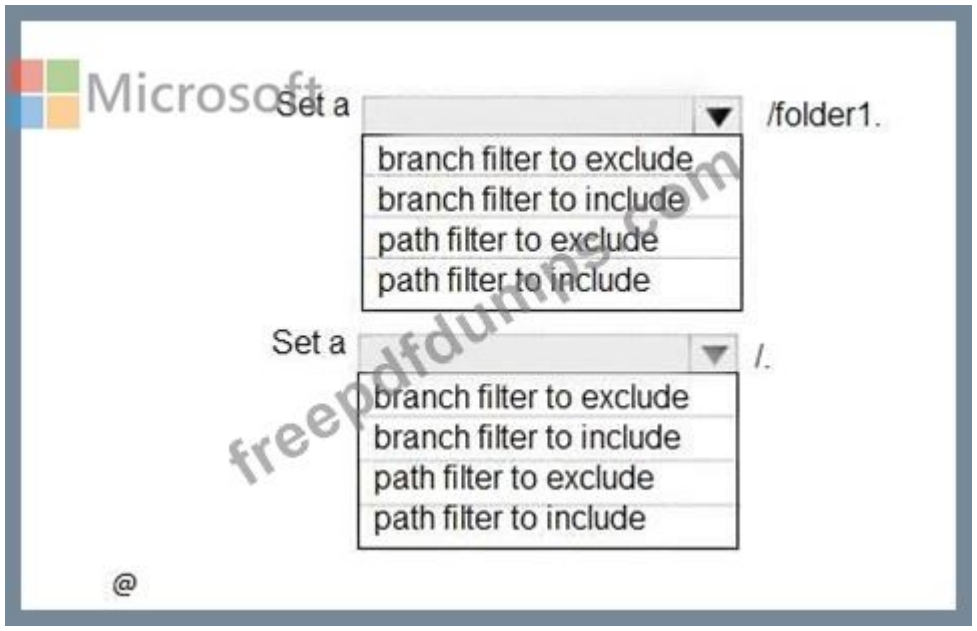
References:
https://docs.sonarqube.org/display/SCAN/Analyzing+with+SonarQube+Extension+for+VSTS-TFS

NEW QUESTION: 103
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 an agent pool.

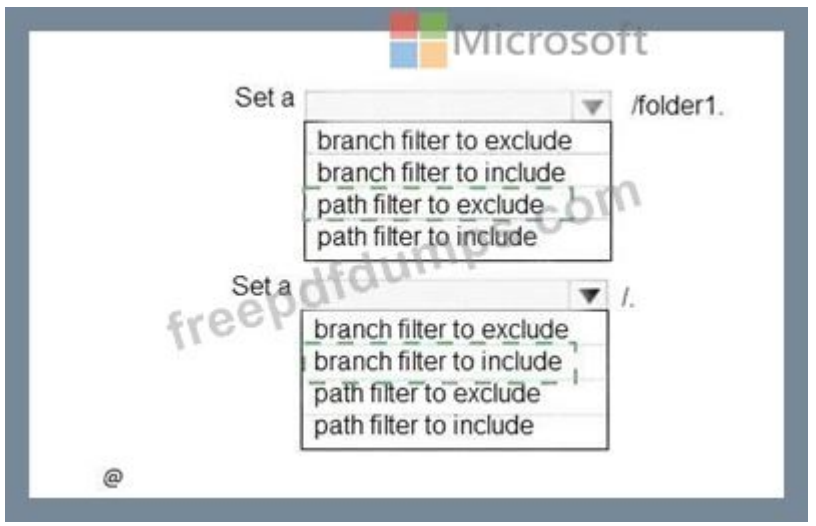
C. Create a deployment group.
D. Reduce the size of the repository.
E. Increase the number of parallel jobs.
Answer: B,E (LEAVE A REPLY)
Question I need more hosted build resources. What can I do?
Answer The Azure Pipelines pool provides all Azure DevOps organizations with cloud-hosted build agents and 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.
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

NEW QUESTION: 104
You are monitoring the health and performance of an Azure web app by using Azure Application Insights. You need to ensure that an alert is sent when the web app has a sudden rise in performance issues and failures. What should you use?
A. Application Insights Profiler
B. Smart Detection
C. usage analysis
D. custom events
E. Continuous export
Answer: B (LEAVE A REPLY)

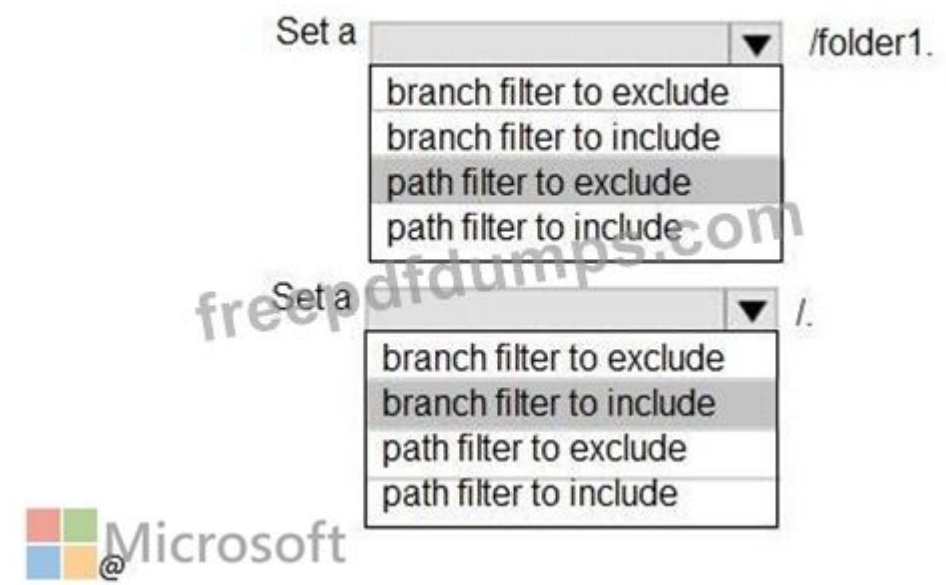
NEW QUESTION: 105
How should you configure the filters for the Project5 trigger? To answer, select the appropriate option in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation



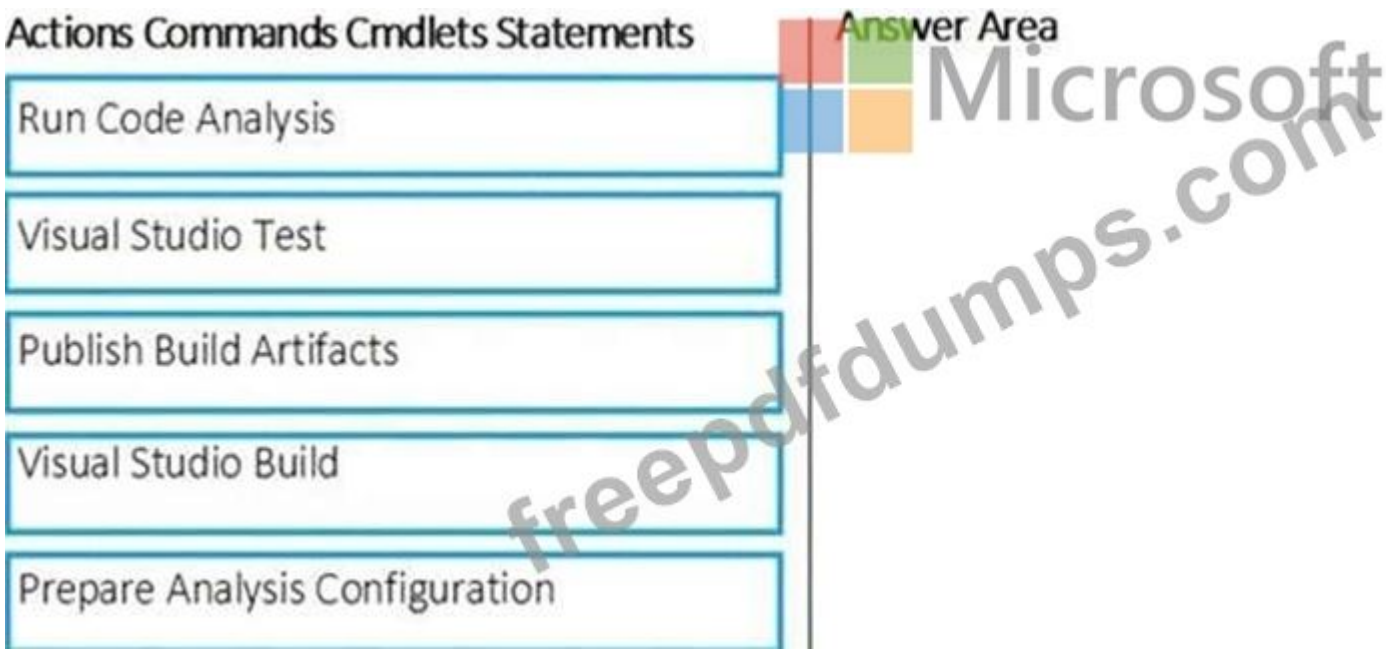
Scenario:

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

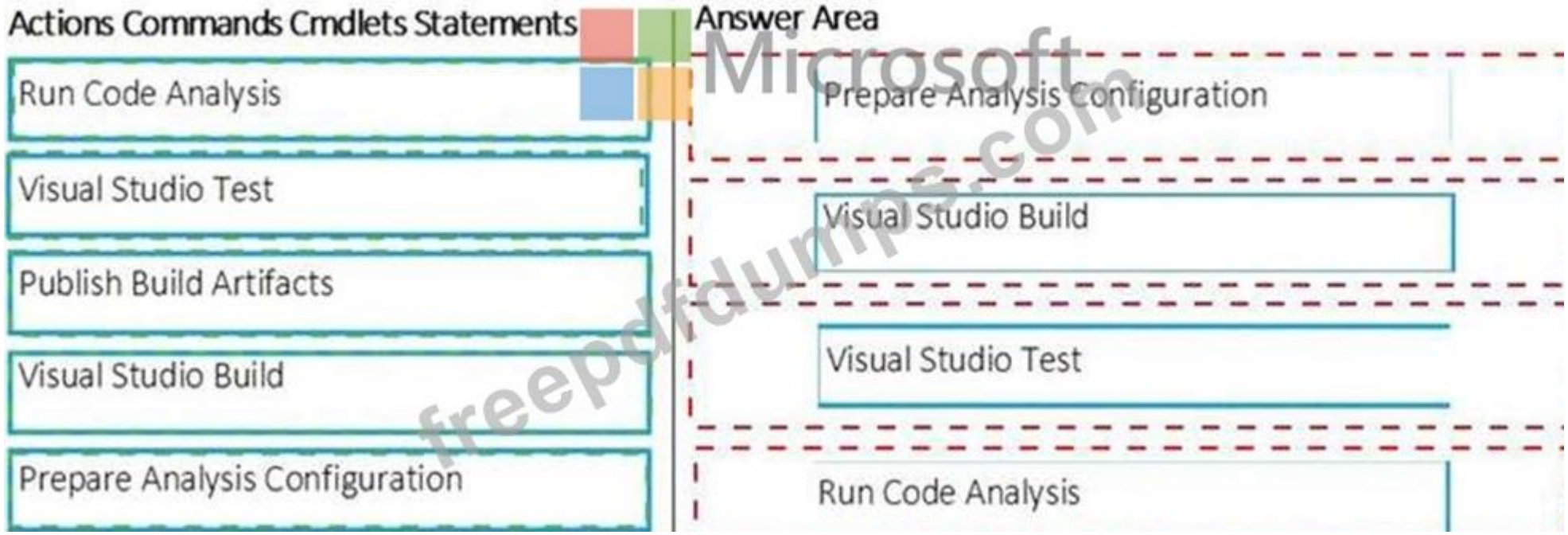
NEW QUESTION: 106
Your company uses cloud-hosted Jenkins for builds.
You need to ensure that Jenkins can retrieve source code from Azure Repos.
Which three actions should you perform? Each correct answer presents part of the solution NOTE: Each correct answer selection is worth one point
A. Add the Team Foundation Server (TFS) plug-in to Jenkins.
B. Create a personal access token m your Azure DevOps account.
C. Create a webhook in Jenkins.
D. Add a domain to your Jenkins account.
E. Create a service hook m Azure DevOps.
Answer: (SHOW ANSWER)
References:
https://blogs.msdn.microsoft.com/devops/2017/04/25/vsts-visual-studio-team-services-integration-with-jenkins/
http://www.aisoftwarellc.com/blog/post/how-to-setup-automated-builds-using-jenkins-and-visual-studio-team-foundation-server/2044

NEW QUESTION: 107
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. Azure virtual machines
B. an Azure virtual machine scale set
C. an Azure Kubernetes Service (AKS) cluster
D. Azure Container Instances
Answer: (SHOW ANSWER)
Explanation
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops&tabs=browser#faq

NEW QUESTION: 108
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.



Answer:



Explanation

Step 1: Prepare Analysis Configuration

Prepare Analysis Configuration task, to configure all the required settings before executing the build.

This task is mandatory.

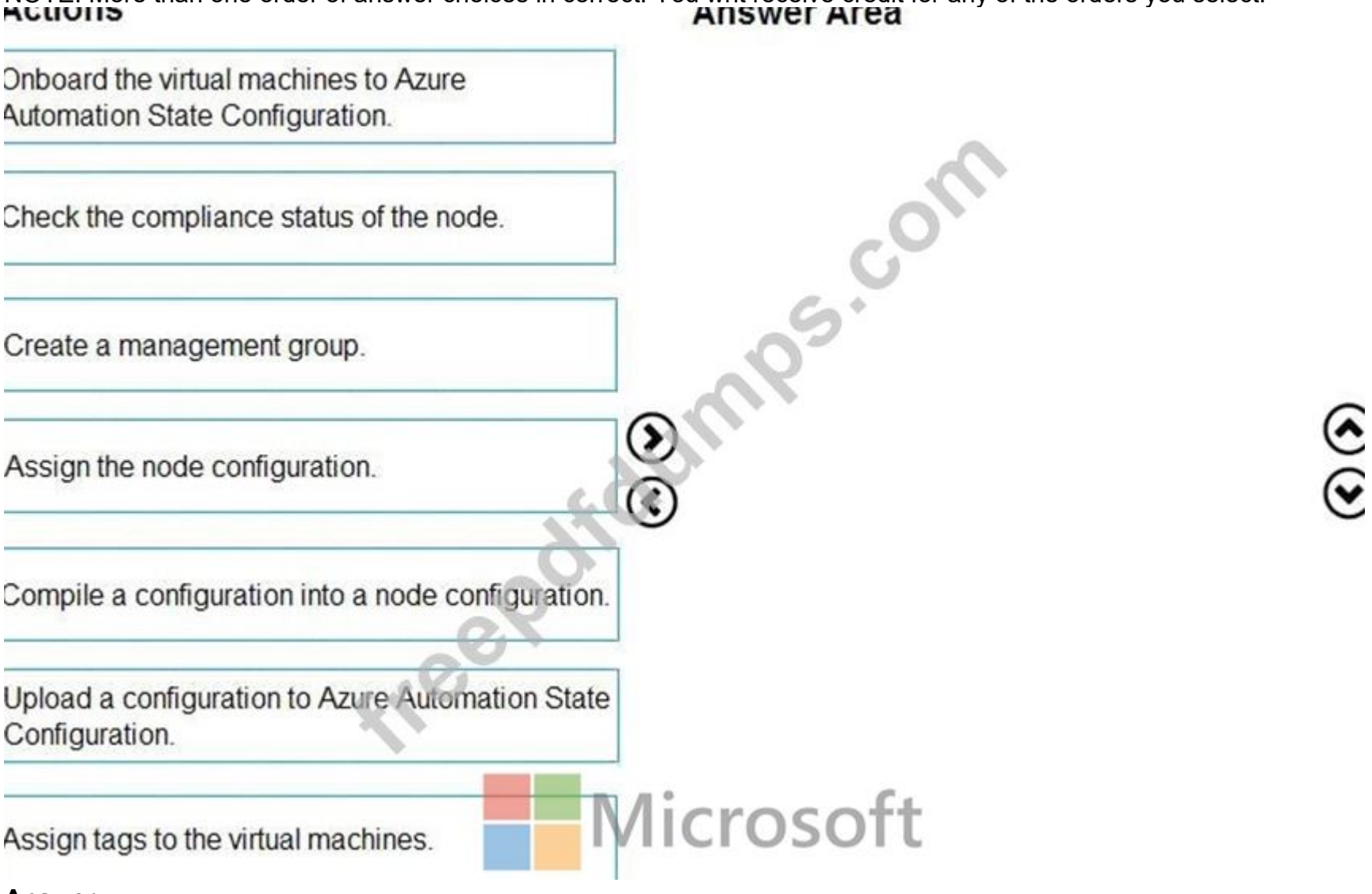
In case of .NET solutions or Java projects, it helps to integrate seamlessly with MSBuild, Maven and Gradle tasks.
Step 2: Visual Studio Build
Reorder the tasks to respect the following order:
Prepare Analysis Configuration task before any MSBuild or Visual Studio Build task.
Step 3: Visual Studio Test
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

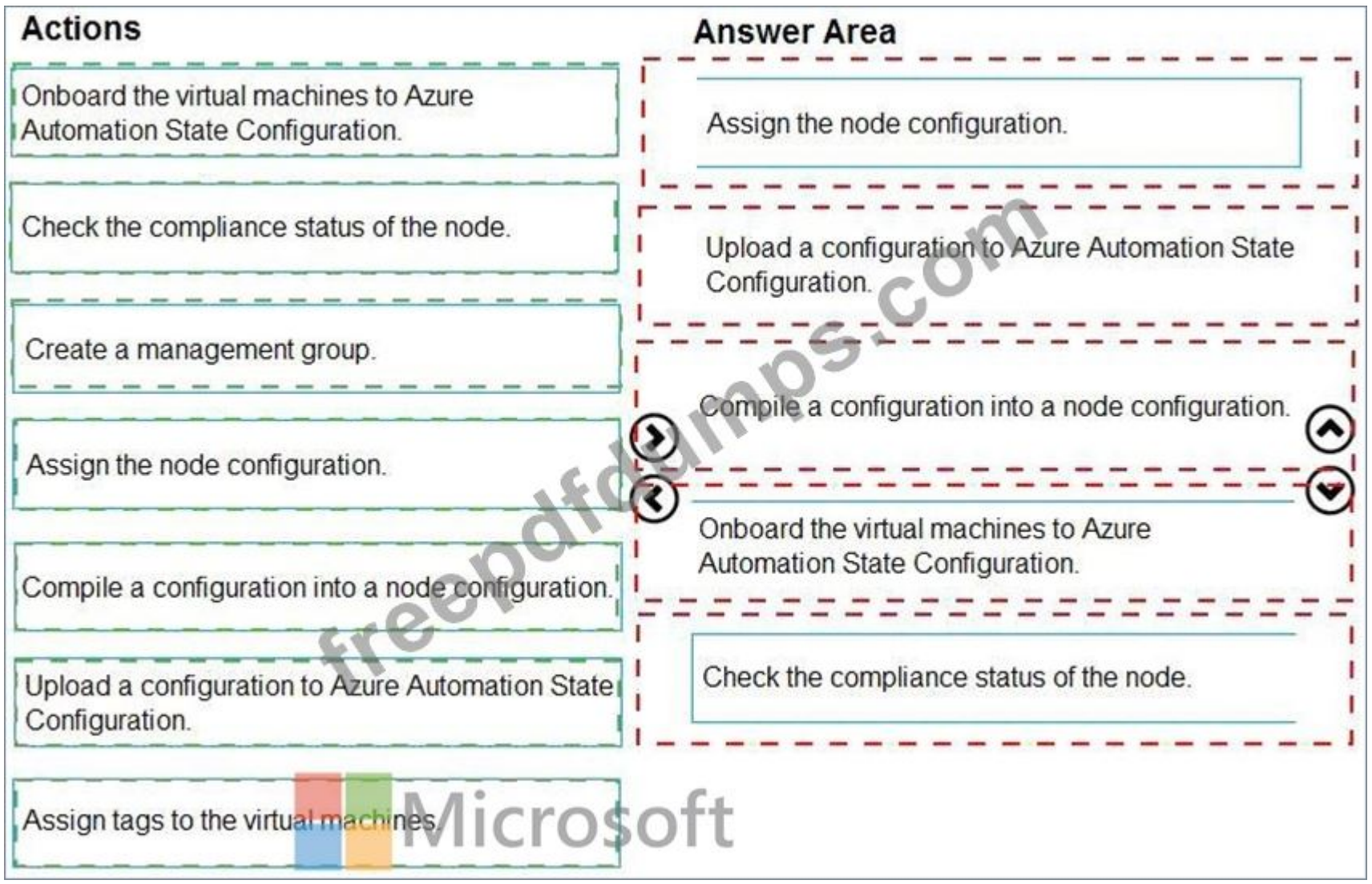
NEW QUESTION: 109
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You 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 (LEAVE A REPLY)
Instead implement Continuous Assurance for the project.
Reference:
https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html

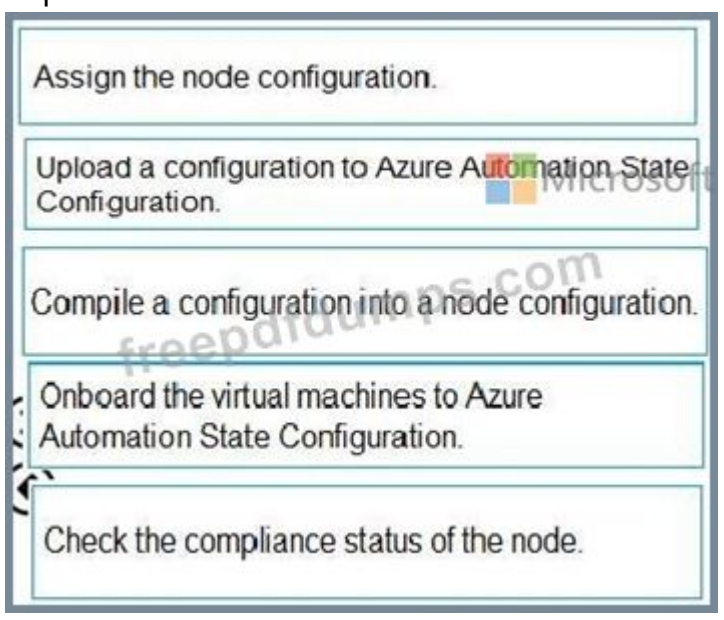
NEW QUESTION: 110
You need to use Azure Automation Sure Configuration to manage the ongoing consistency of virtual machine configurations.
Which five actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
NOTE: More than one order of answer choices in correct. You writ receive credit for any of the orders you select.



Answer:



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

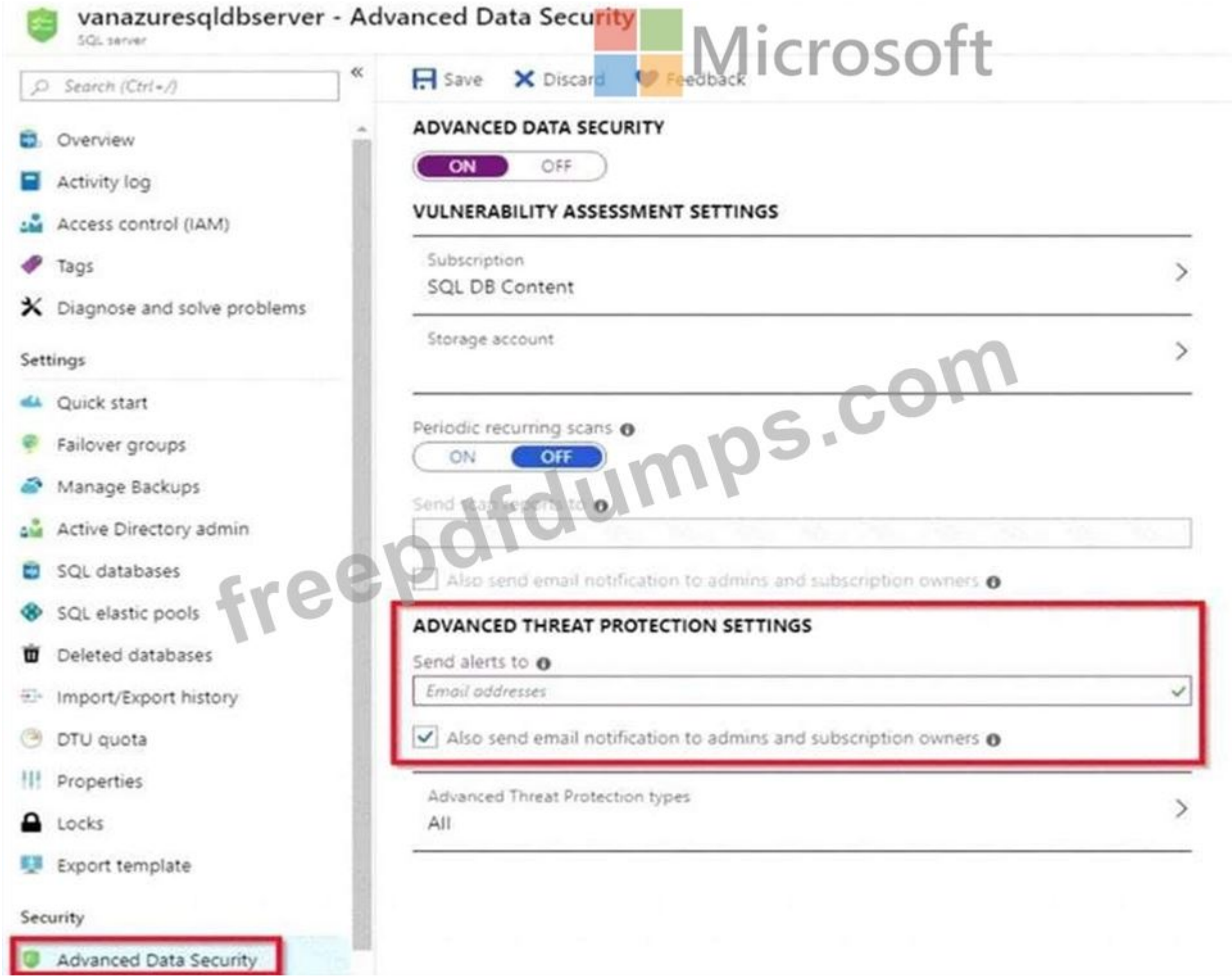
NEW QUESTION: 111
You have a web app hosted on Azure App Service. The web app stores data in an Azure SQL database.
You need to generate an alert when there are 10,000 simultaneous connections to the database. The solution must minimize deve4opment effort.
Which option should you select in the Diagnostics settings of the database?
A. Send to Log Analytics
B. Stream to an event hub
C. Archive to m storage account
Answer: (SHOW ANSWER)

NEW QUESTION: 112
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You 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 (LEAVE A REPLY)
The basic idea behind Continuous Assurance (CA) is to setup the ability to check for "drift" from what is considered a secure snapshot of a system. Support for Continuous Assurance lets us treat security truly as a
'state' as opposed to a 'point in time' achievement. This is particularly important in today's context when
'continuous change' has become a norm.
There can be two types of drift:
* Drift involving 'baseline' configuration: This involves settings that have a fixed number of possible states (often pre-defined/statically determined ones). For instance, a SQL DB can have TDE encryption turned ON or OFF...or a Storage Account may have auditing turned ON however the log retention period may be less than 365 days.

* Drift involving 'stateful' configuration: There are settings which cannot be constrained within a finite set of well-known states. For instance, the IP addresses configured to have access to a SQL DB can be any (arbitrary) set of IP addresses. In such scenarios, usually human judgment is initially required to determine whether a particular configuration should be considered 'secure' or not. However, once that is done, it is important to ensure that there is no "stateful drift" from the attested configuration. (E.g., if, in a troubleshooting session, someone adds the IP address of a developer machine to the list, the Continuous Assurance feature should be able to identify the drift and generate notifications/alerts or even trigger 'auto- remediation' depending on the severity of the change).
Reference:
https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html

NEW QUESTION: 113
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
Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

NEW QUESTION: 114
You manage a website that uses an Azure SQL Database named db1 in a resource group named RG1lod11566895.
You need to modify the SQL database to protect against SQL injection.
To complete this task, sign in to the Microsoft Azure portal.
Answer:
See solution below.
Explanation
Set up Advanced Threat Protection in the Azure portal
1. Sign into the Azure portal.
2. Navigate to the configuration page of the server you want to protect. In the security settings, select Advanced Data Security.
3. On the Advanced Data Security configuration page:



4. Enable Advanced Data Security on the server.

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

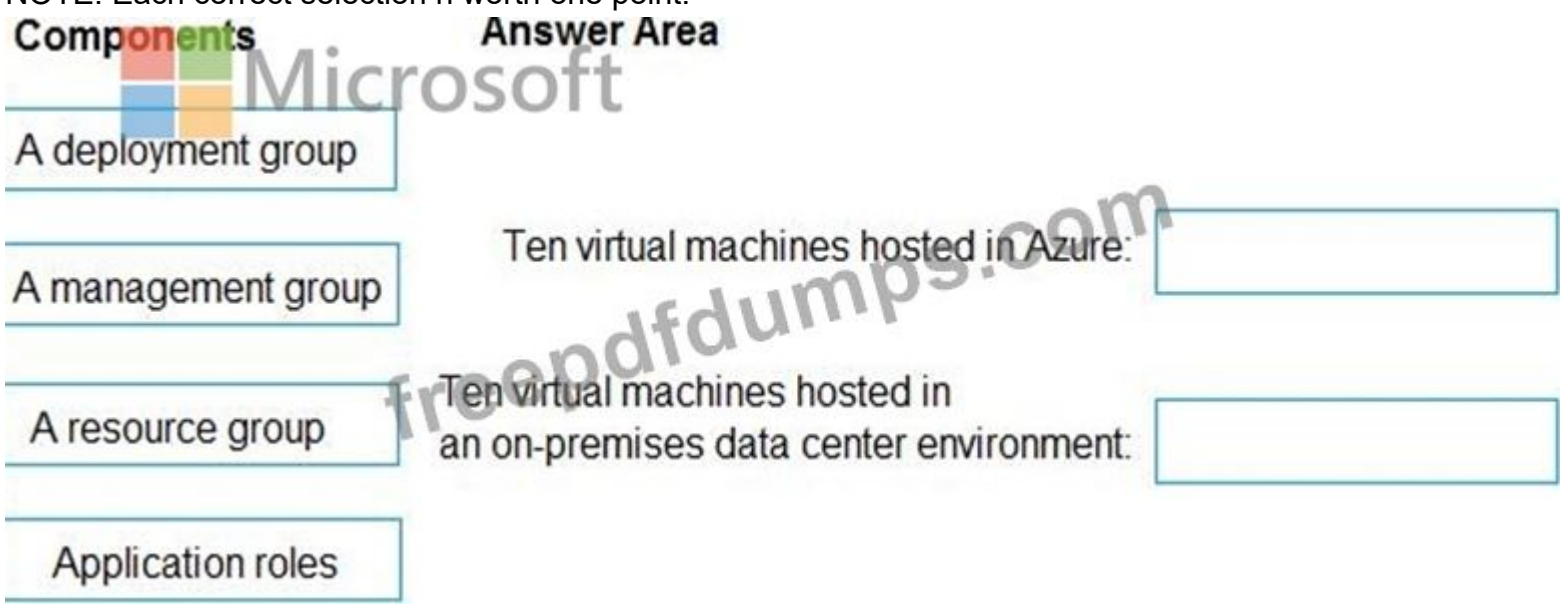
https://docs.microsoft.com/en-us/azure/storage/common/storage-account-create

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

NEW QUESTION: 115

Your company plans to deploy an application to the following endpoints:

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

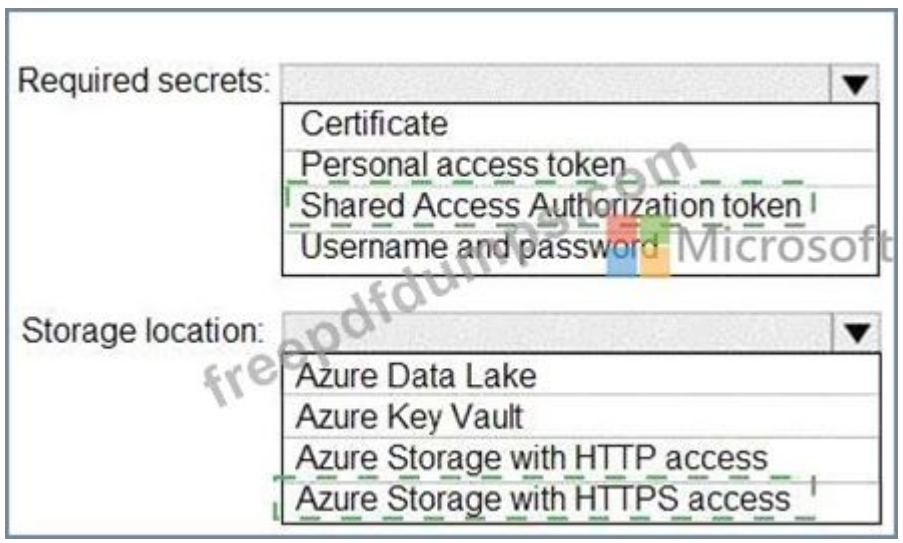


Answer:

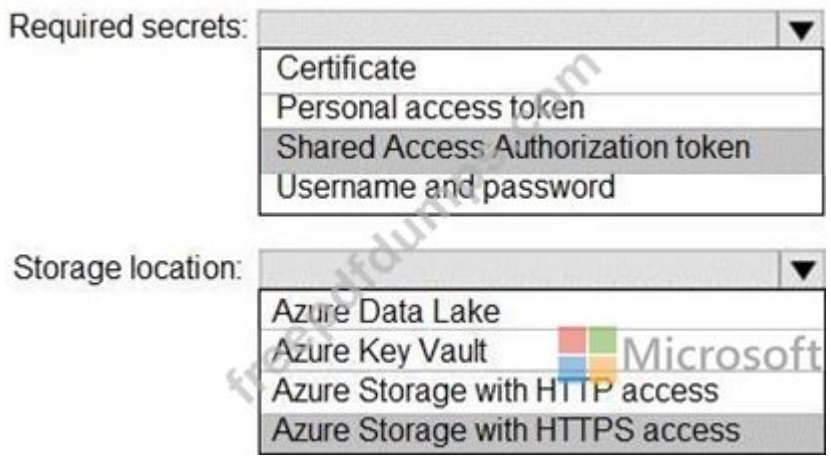
Explanation:
Box 1: A deployment group
When authoring an Azure Pipelines or TFS Release pipeline, you can specify the deployment targets for a job using a deployment group.
If the target machines are Azure VMs, you can quickly and easily prepare them by installing the Azure Pipelines Agent Azure VM extension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

NEW QUESTION: 116
You need to configure a cloud service to store the secrets required by the mobile applications to call the share.
What should you include in the solution? To answer, select the appropriate options m the answer ate, NOTE:
Each correct selection is worth one point.

Answer:



Explanation



Every request made against a storage service must be authorized, unless the request is for a blob or container resource that has been made available for public or signed access. One option for authorizing a request is by using Shared Key.

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

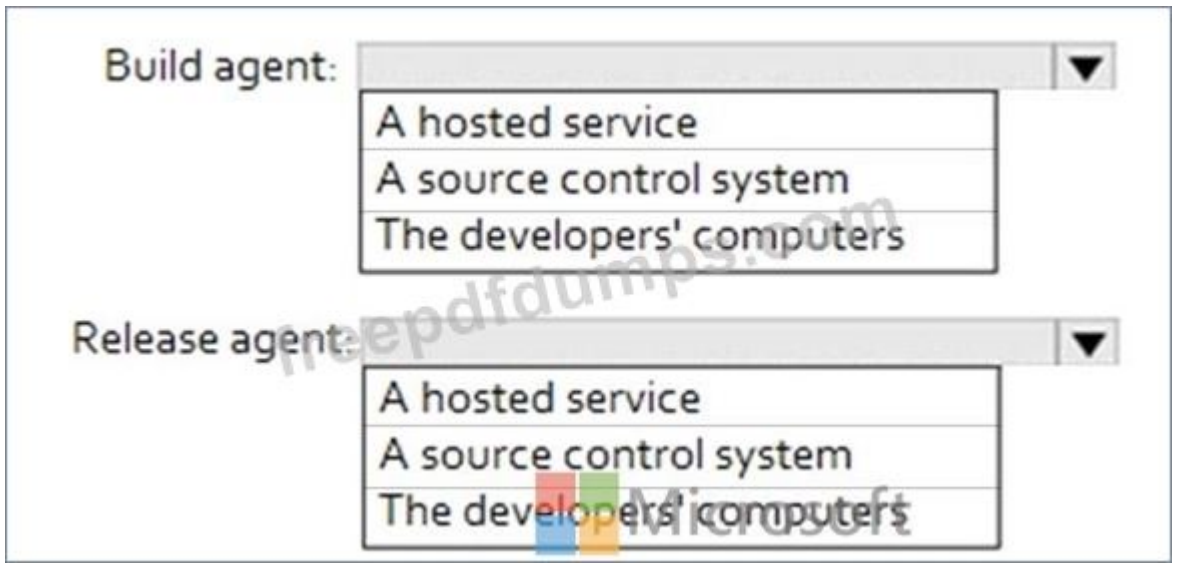
The investment planning applications suite will include one multi-tier web application and two iOS mobile application. One mobile application will be used by employees; the other will be used by customers.

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

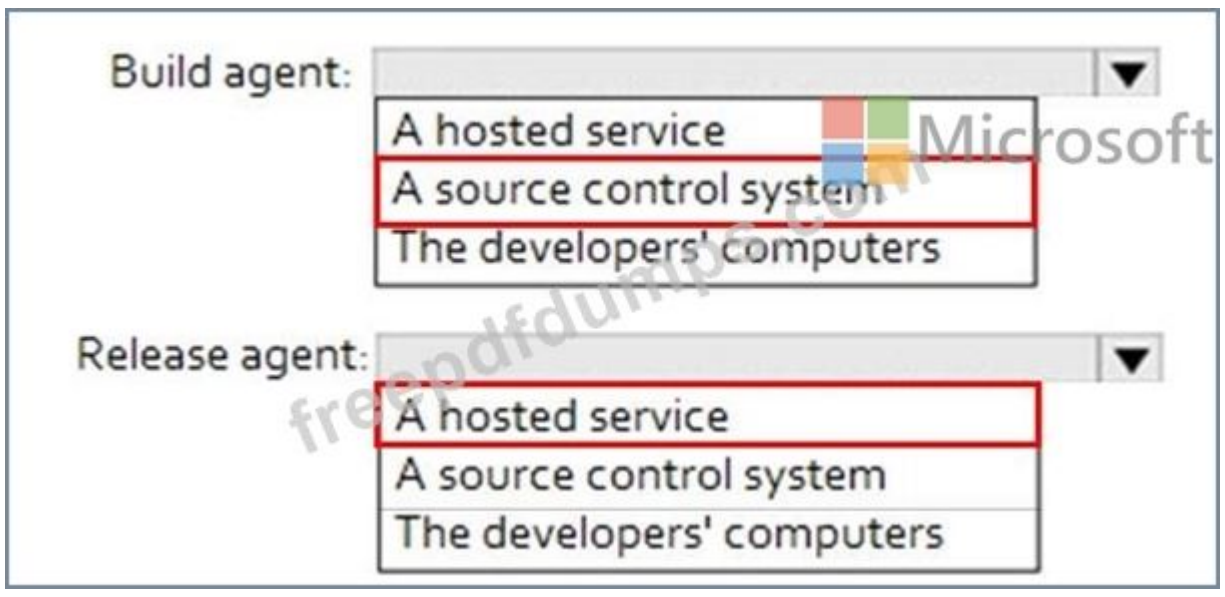
NEW QUESTION: 117

Where should the build and release agents for the investment planning application suite run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Box 1: A source control system

A source control system, also called a version control system, allows developers to collaborate on code and track changes. Source control is an essential tool for multi-developer projects.

Box 2: A hosted service

To build and deploy Xcode apps or Xamarin.iOS projects, you'll need at least one macOS agent. If your pipelines are in Azure Pipelines and a Microsoft-hosted agent meets your needs, you can skip setting up a self-hosted macOS agent.

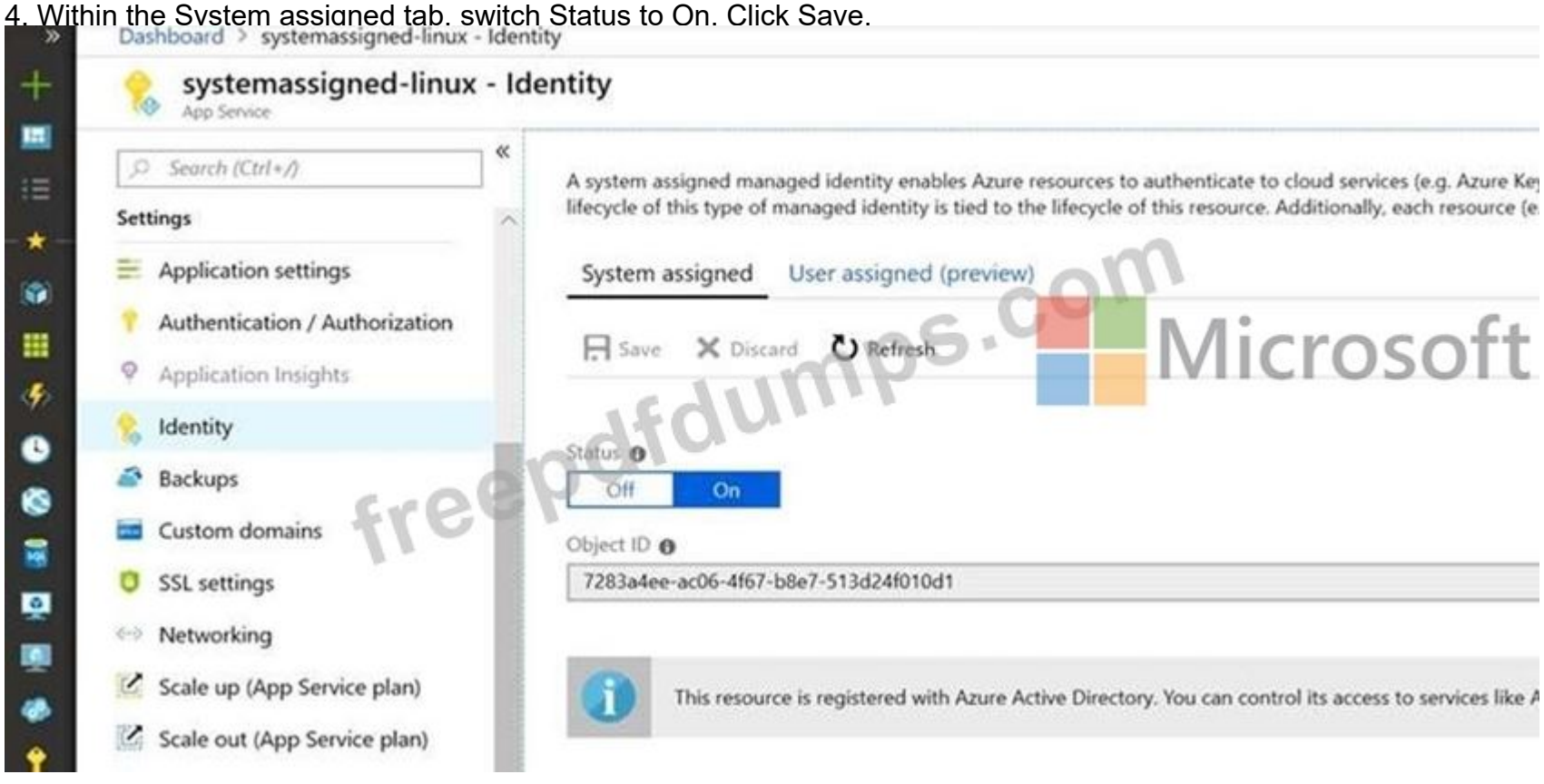
Scenario: The investment planning applications suite will include one multi-tier web application and two iOS mobile applications. One mobile application will be used by employees; the other will be used by customers.

References:

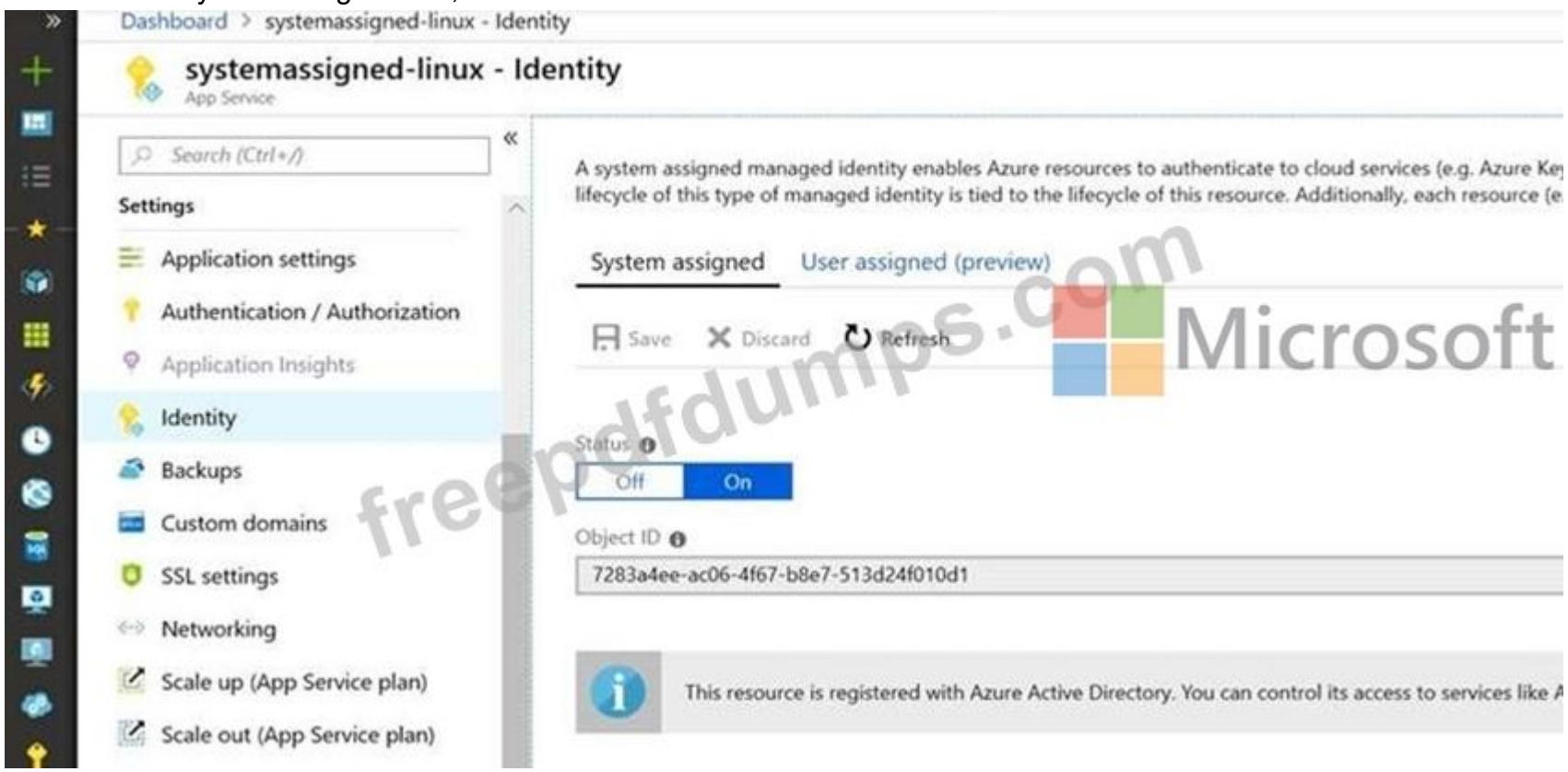
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-osx?view=azure-devops

NEW QUESTION: 118
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. Increase the number of parallel jobs.
B. Move to a blue/green deployment pattern.
C. Reduce the size of the repository.
D. Create an agent pool.
E. Create a deployment group.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 119
SIMULATION
You need to ensure that an Azure web app named az400-9940427-main can retrieve secrets from an Azure key vault named az400-9940427-kv1 by using a system managed identity.
The solution must use the principle of least privilege.
To complete this task, sign in to the Microsoft Azure portal.
A. 1. In Azure portal navigate to the az400-9940427-main app.
2. Scroll down to the Settings group in the left navigation.
3. Select Managed identity.
4. Within the System assigned tab, switch Status to On. Click Save.



B. 1. In Azure portal navigate to the az400-9948427-main app.
2. Scroll down to the Settings group in the left navigation.
3. Within the System assigned tab, switch Status to On. Click Save.



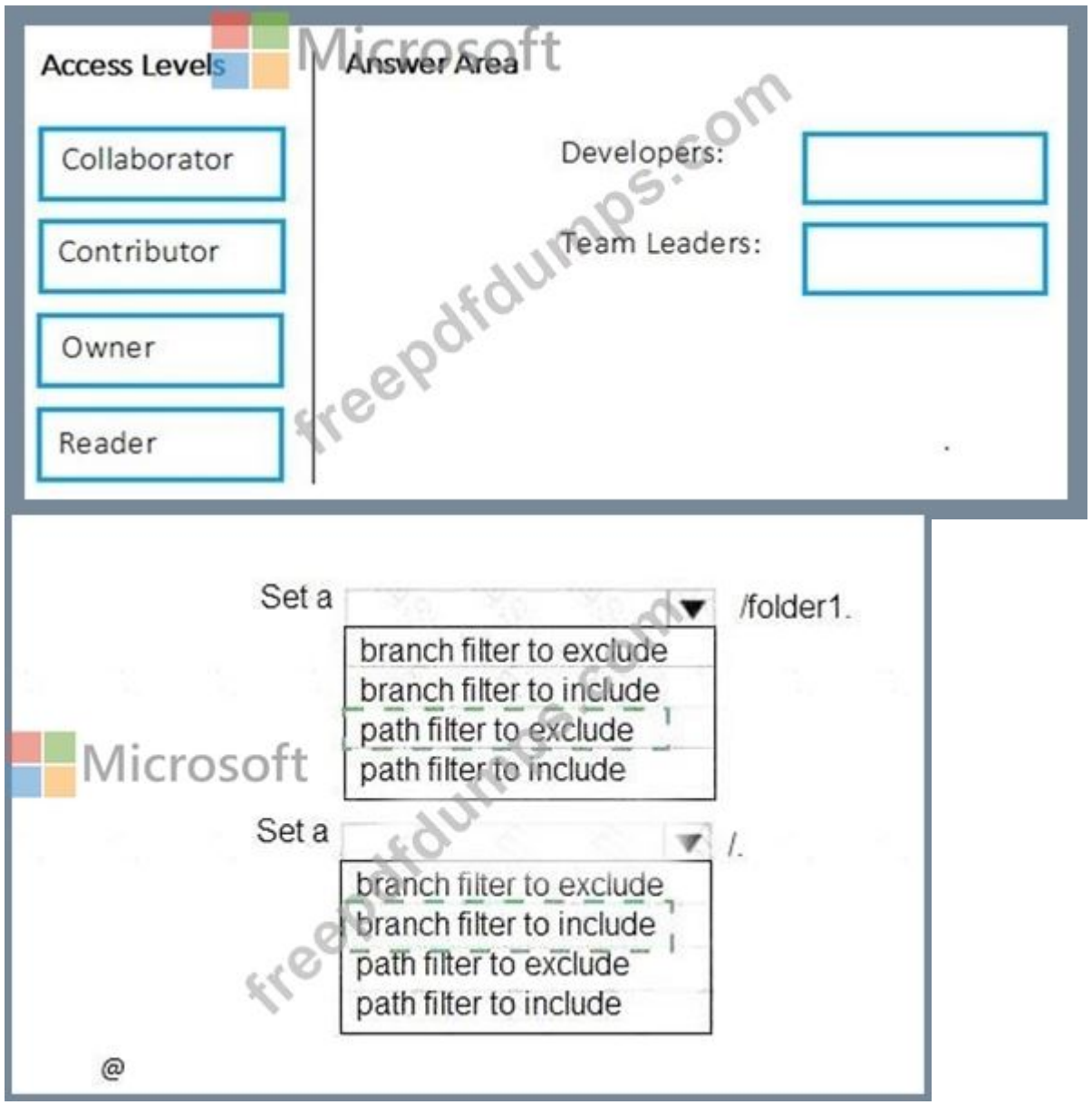
Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 120
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. Create a membership database in an Azure SQL database.
B. Assign an enterprise application to users and groups.
C. Create an app registration in Azure AD.
D. Configure the application to use a SAML endpoint.
E. Create a new OAuth token from the application.
Answer: C (LEAVE A REPLY)
Explanation
Register your application to use Azure Active Directory. Registering the application means that your developers can use Azure AD to authenticate users and request access to user resources such as email, calendar, and documents.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/developer-guidance-for-integrating-applica

NEW QUESTION: 121
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.



Explanation

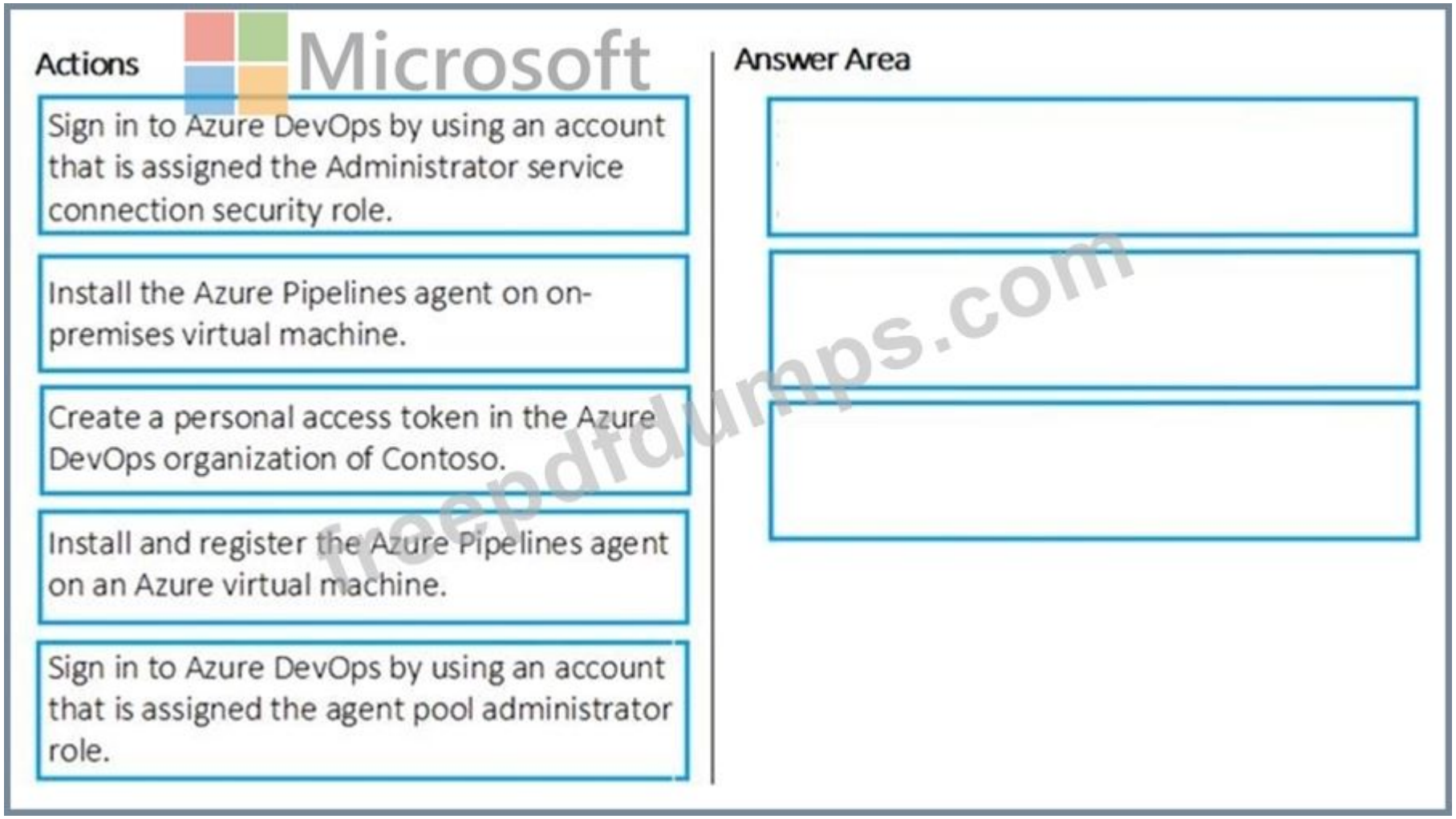
Box 1: Reader
Members of a group named Developers must be able to install packages.
Feeds have four levels of access: Owners, Contributors, Collaborators, and Readers. Owners can add any type of identity-individuals, teams, and groups-to any access level.
Box 2: Owner
Members of a group named Team Leaders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

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

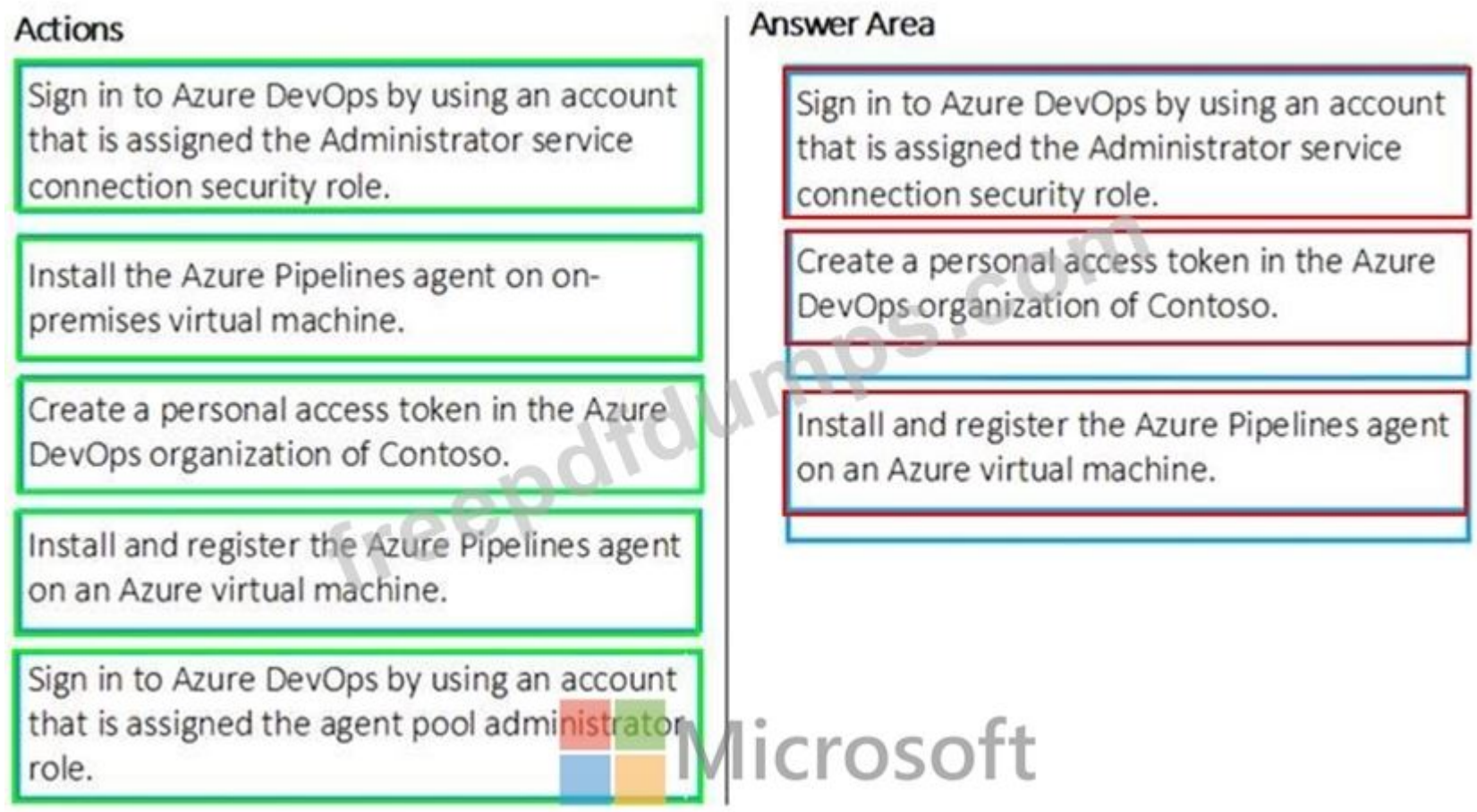
NEW QUESTION: 122

You need to recommend a procedure to implement the build agent for Project1.

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


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

Answer:


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

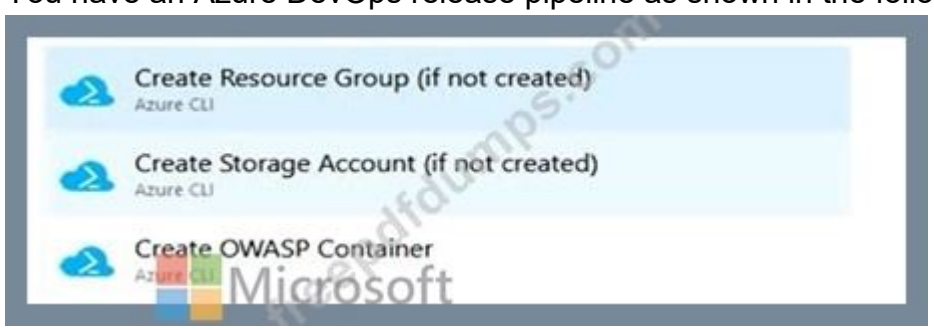
Explanation:
Scenario:

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

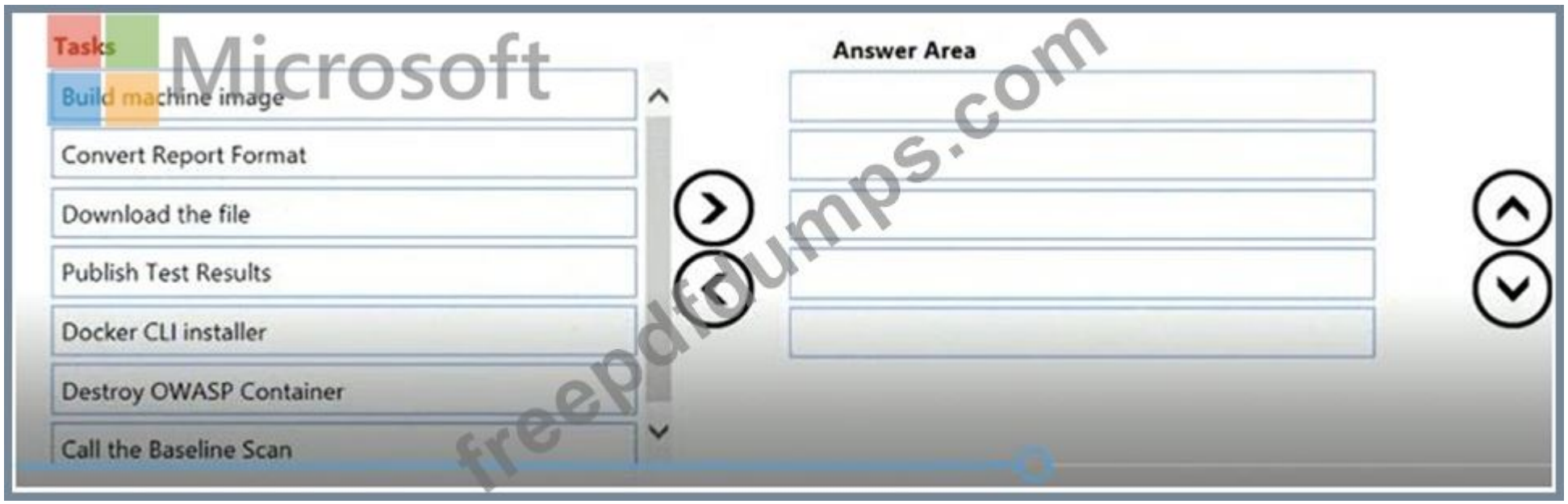
Step 1: Sign in to Azure Devops by using an account that is assigned the Administrator service connection security role.
Note: Under Agent Phase, click Deploy Service Fabric Application. Click Docker Settings and then click Configure Docker settings. In Registry Credentials Source, select Azure Resource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

NEW QUESTION: 123
You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 and an Azure Standard Load Balancer named LB1.
LB1 distributes incoming requests across VMSS1 instances.
You use Azure DevOps to build a web app named Appl and deploy App1 to VMSS1. App1 is accessible via HTTPS only and configured to require mutual authentication by using a client certificate.
You need to recommend a solution for implementing a health check of App1. The solution must meet the following requirements:
* Identify whether individual instances of VMSSI are eligible for an upgrade operation.
* Minimize administrative effort.
What should you include in the recommendation?
A. an Azure Load Balancer health probe
B. the Custom Script Extension
C. Azure Monitor autoscale
D. the Application Health extension
Answer: A (LEAVE A REPLY)

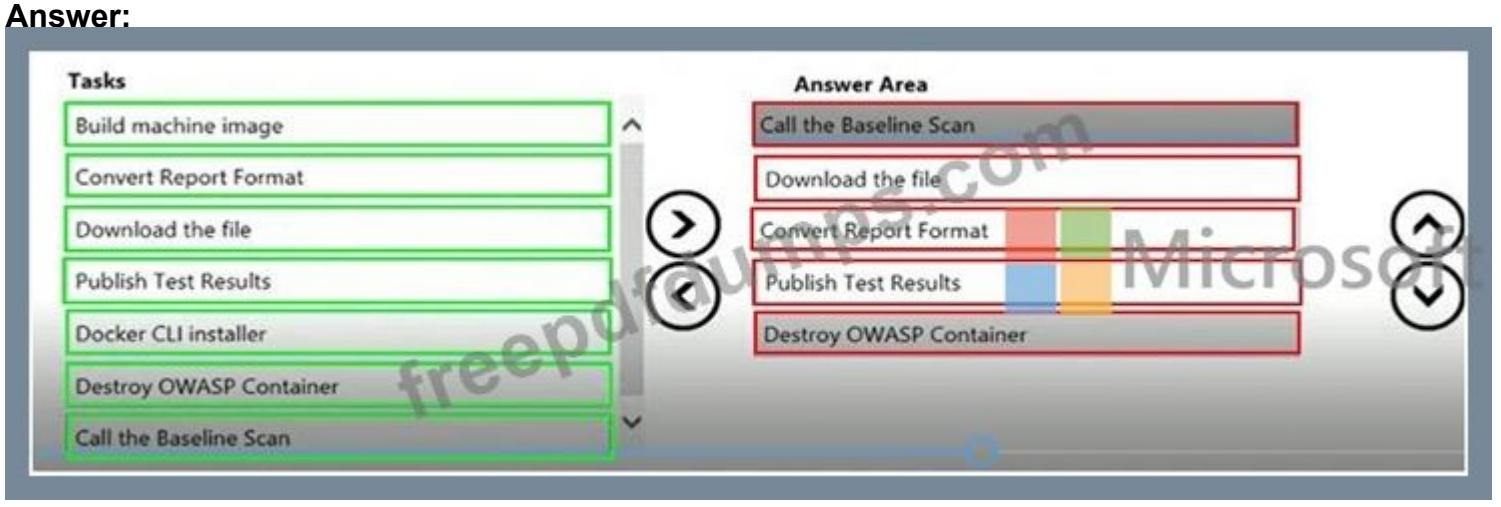
NEW QUESTION: 124
You have an Azure DevOps release pipeline as shown in the following exhibit.



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.



Answer:



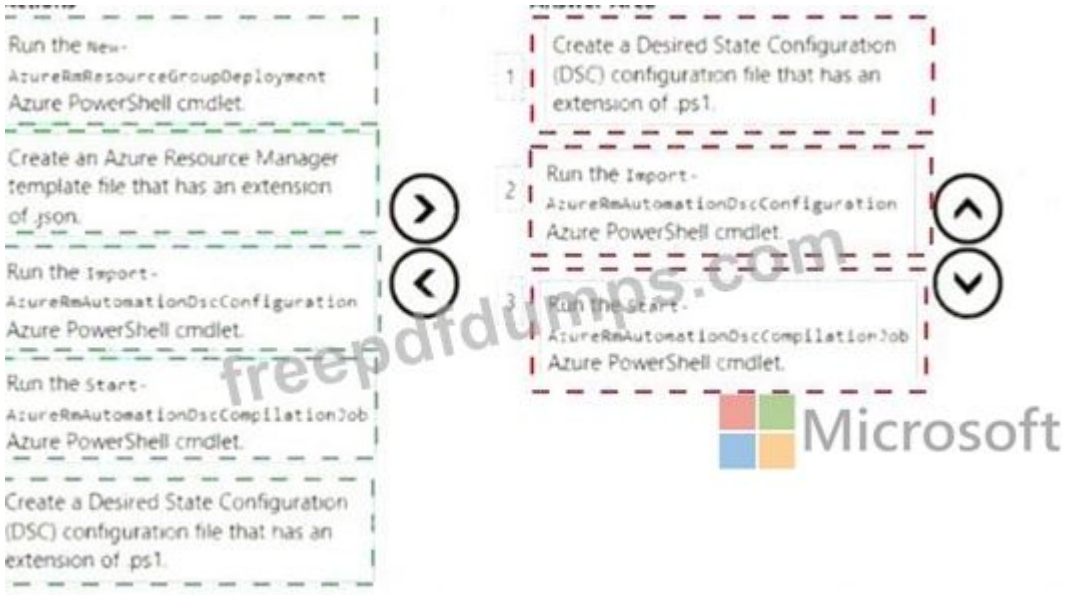
NEW QUESTION: 125

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

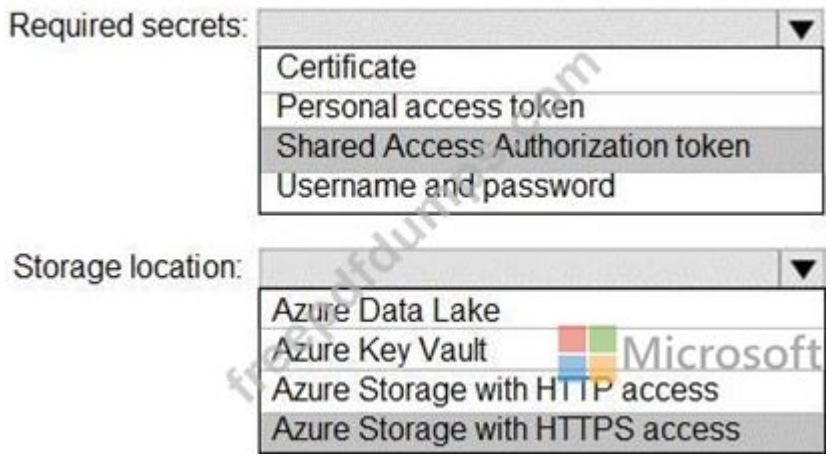
What should you include in the solution? To answer, select the appropriate options m the answer ates, NOTE:

Each correct selection is worth one point.

Answer:



Explanation



Every request made against a storage service must be authorized, unless the request is for a blob or container resource that has been made available for public or signed access. One option for authorizing a request is by using Shared Key.

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

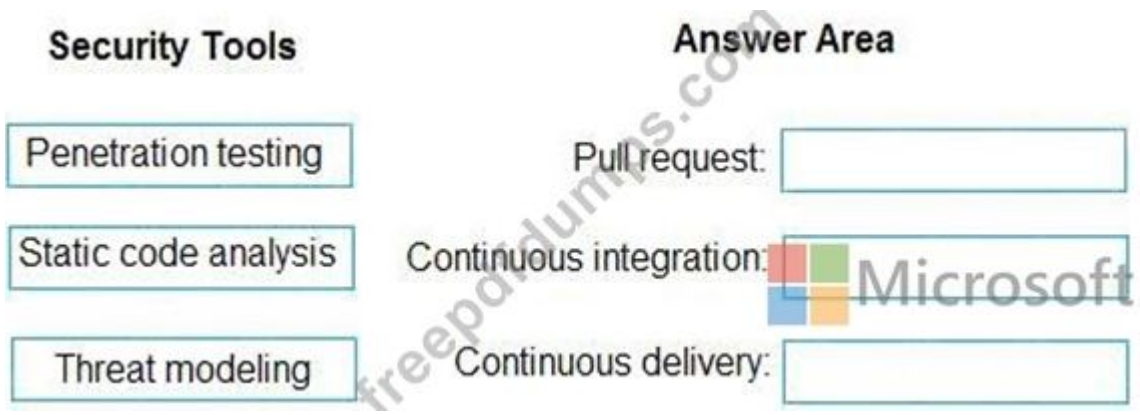
The investment planning applications suite will include one multi-tier web application and two iOS mobile application. One mobile application will be used by employees; the other will be used by customers.

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

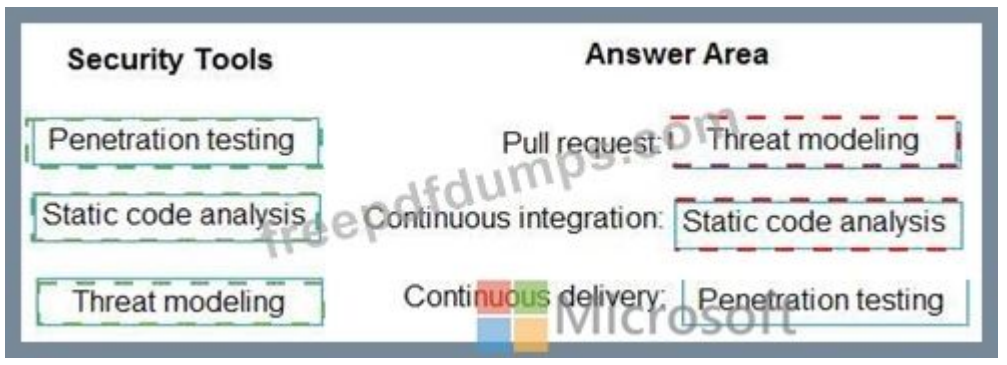
NEW QUESTION: 126

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

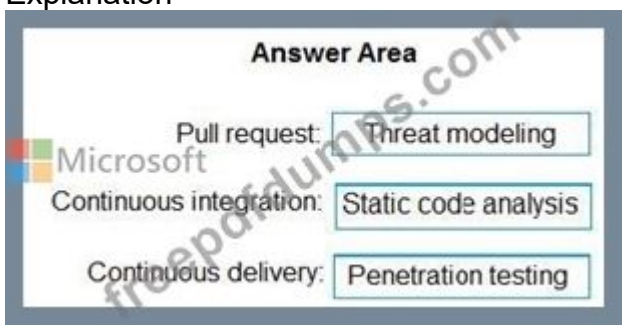
Which type of security tool should you recommend for each stage of the development process? To answer, drag the appropriate security toots to the correct stages. Each security tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content NOTE: Each correct selection is worth one point.



Answer:



Explanation



Box 1: Threat modeling

Threat modeling's motto should be, "The earlier the better, but not too late and never ignore." Box 2: Static code analysis Validation in the CI/CD begins before the developer commits his or her code. Static code analysis tools in the IDE provide the first line of defense to help ensure that security vulnerabilities are not introduced into the CI/CD process.

Box 3: Penetration testing

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

References:

https://docs.microsoft.com/en-us/azure/devops/articles/security-validation-cicd-pipeline?view=vsts

NEW QUESTION: 127

Your company uses Azure Artifacts for package management.

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

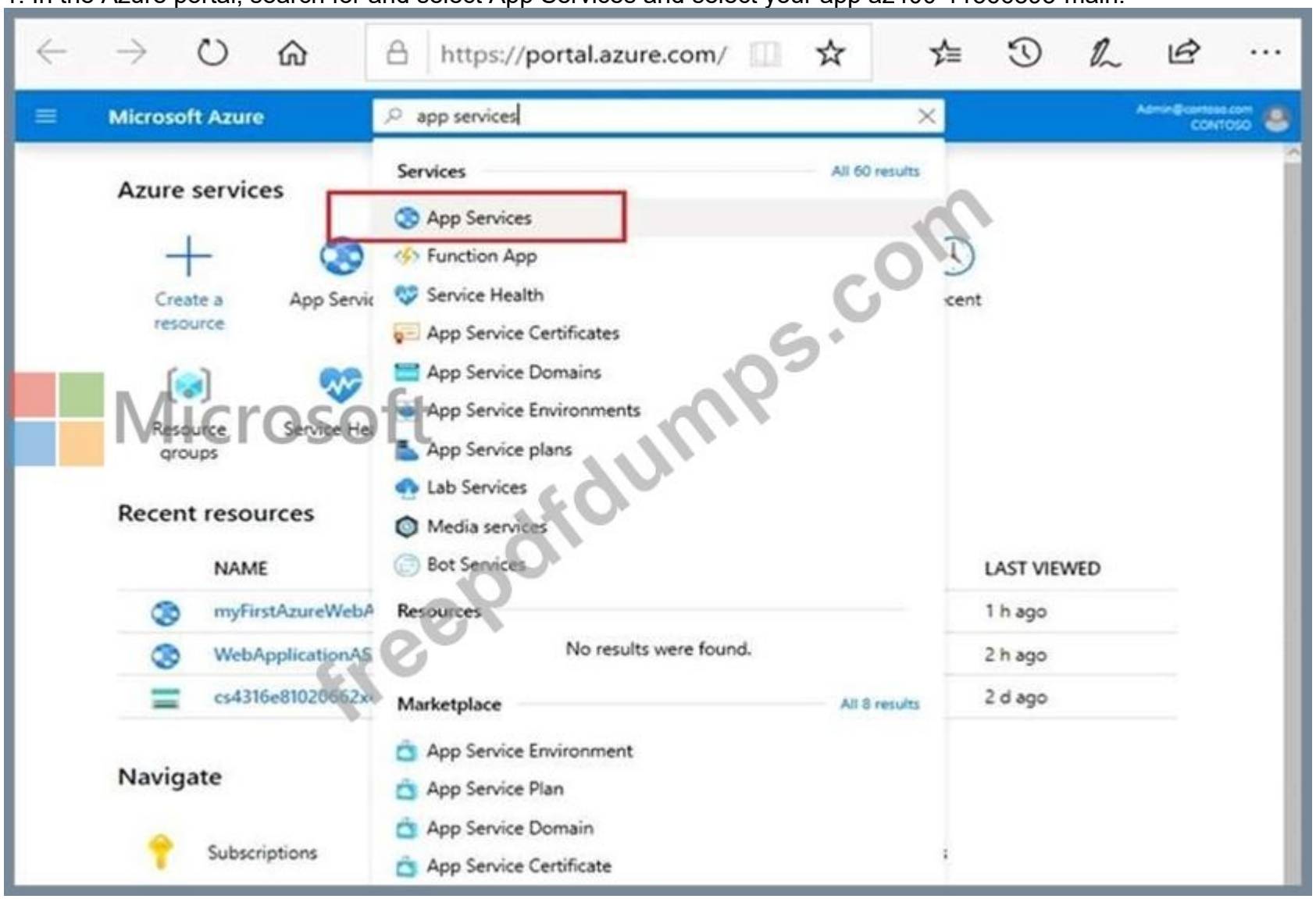
Which repository type should you use as an upstream source?

A. PyPI

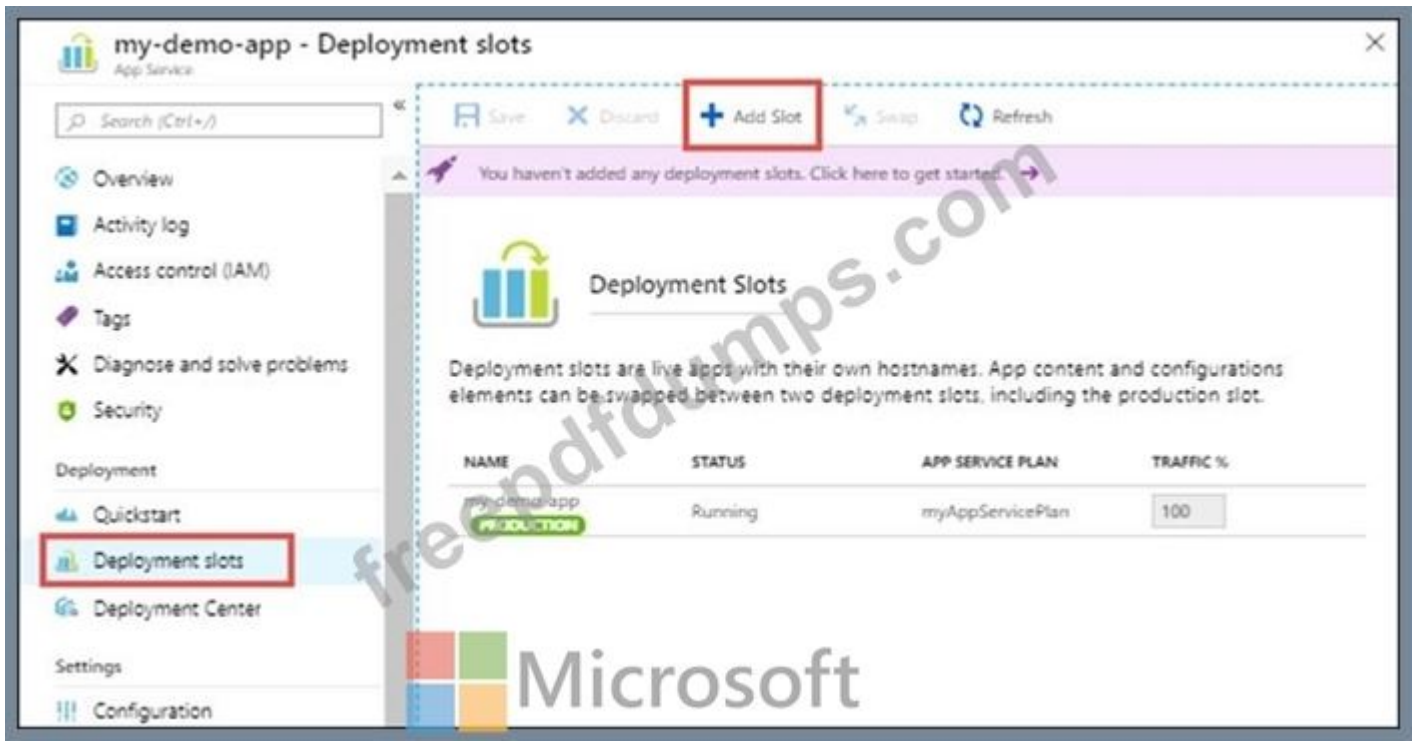
B. third-party trusted Python

C. Maven Central
D. npmjs.org
Answer: (SHOW ANSWER)

NEW QUESTION: 128
You plan to implement a CI/CD strategy for an Azure Web App named az400-11566895-main.
You need to configure a staging environment for az400-11566895-main.
To complete this task, sign in to the Microsoft Azure portal.
A. Add a slot
1. In the Azure portal, search for and select App Services and select your app az400-11566895-main.

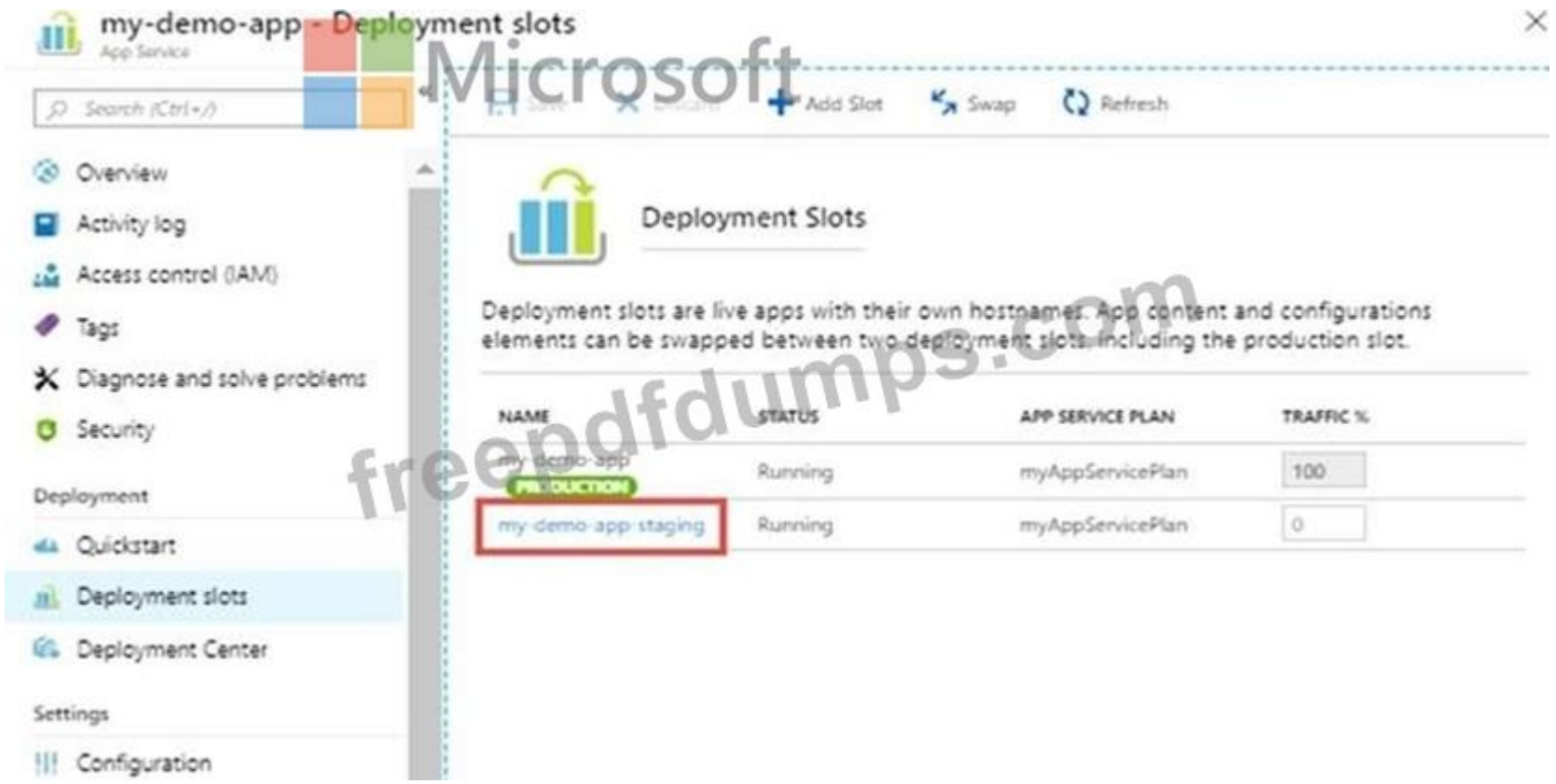


2. In the left pane, select Deployment slots > Add Slot.



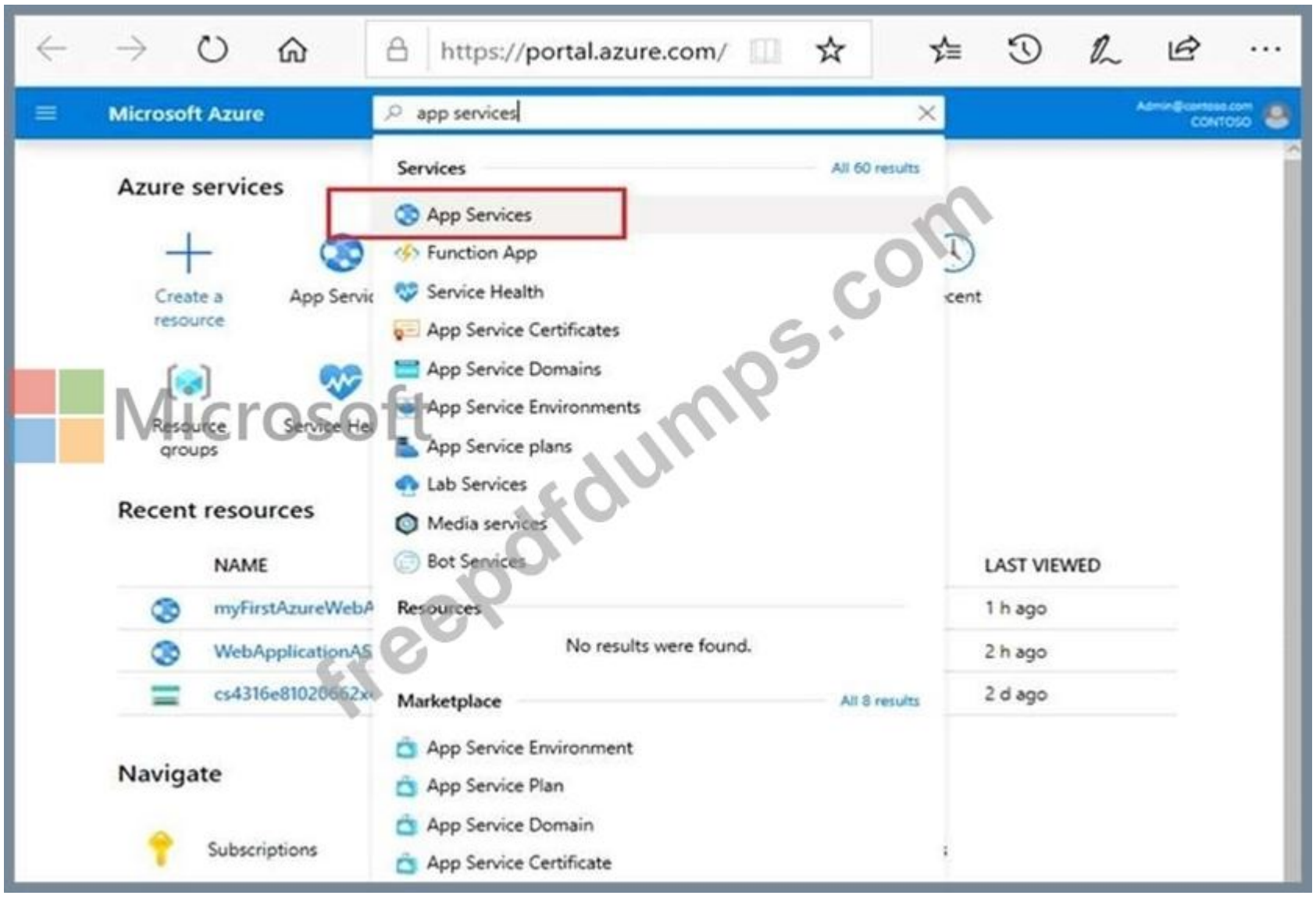
3. In the Add a slot dialog box, give the slot a name, and select whether to clone an app configuration from another deployment slot. Select Add to continue.

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

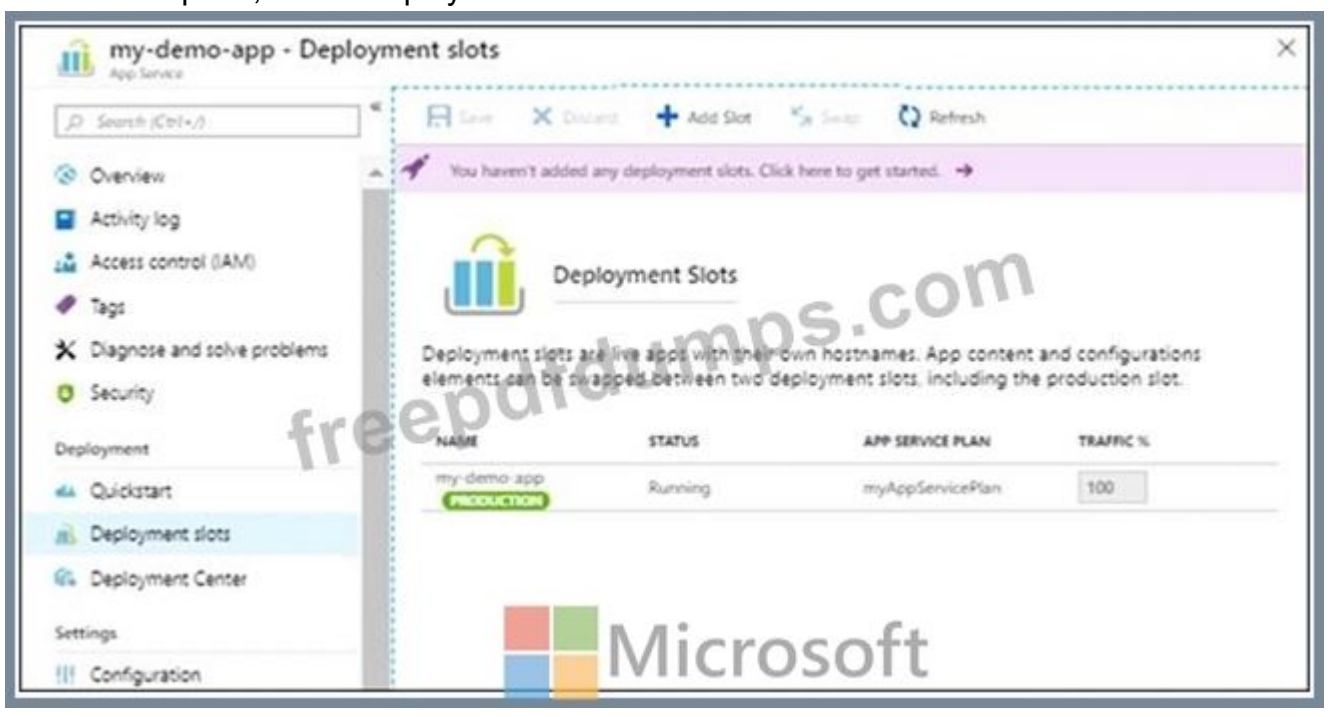


B. Add a slot

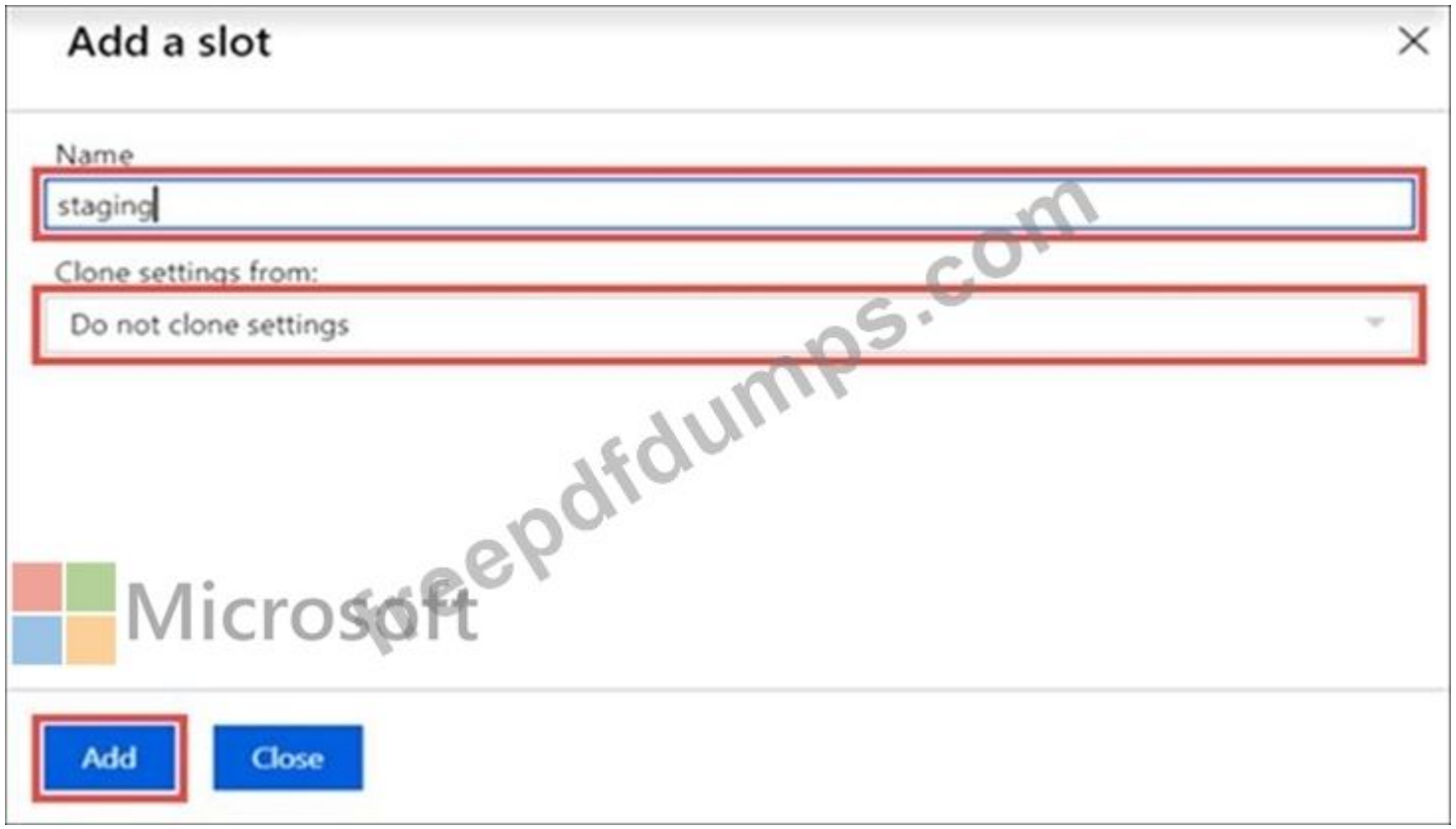
1. In the Azure portal, search for and select App Services and select your app az400-11566895-main.



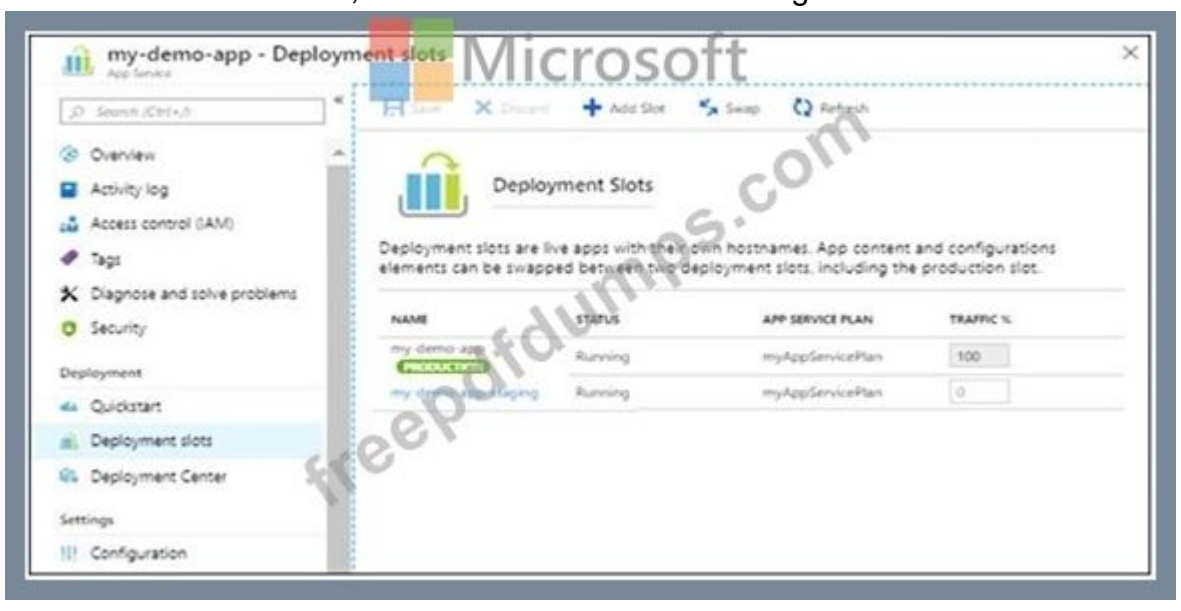
2. In the left pane, select Deployment slots > Add Slot.



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



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



Answer: A (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 129

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 (LEAVE A REPLY)
Explanation
You can import an existing Git repo from GitHub, Bitbucket, GitLab, or other location into a new or empty existing repo in your project in Azure DevOps.
Import into a new repo
* Select Repos, Files.
* From the repo drop-down, select Import repository.
* If the source repo is publicly available, just enter the clone URL of the source repository and a name for your new Git repository.
References:
https://docs.microsoft.com/en-us/azure/devops/repos/git/import-git-repository?view=azure-devops

NEW QUESTION: 130
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: (SHOW ANSWER)
Explanation/Reference:
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

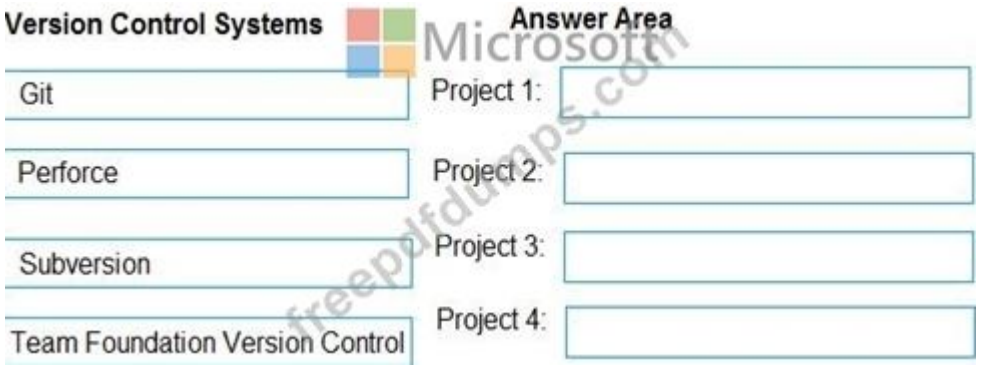
NEW QUESTION: 131
Your company has four projects. The version control requirements for each project are shown in the following table.

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.

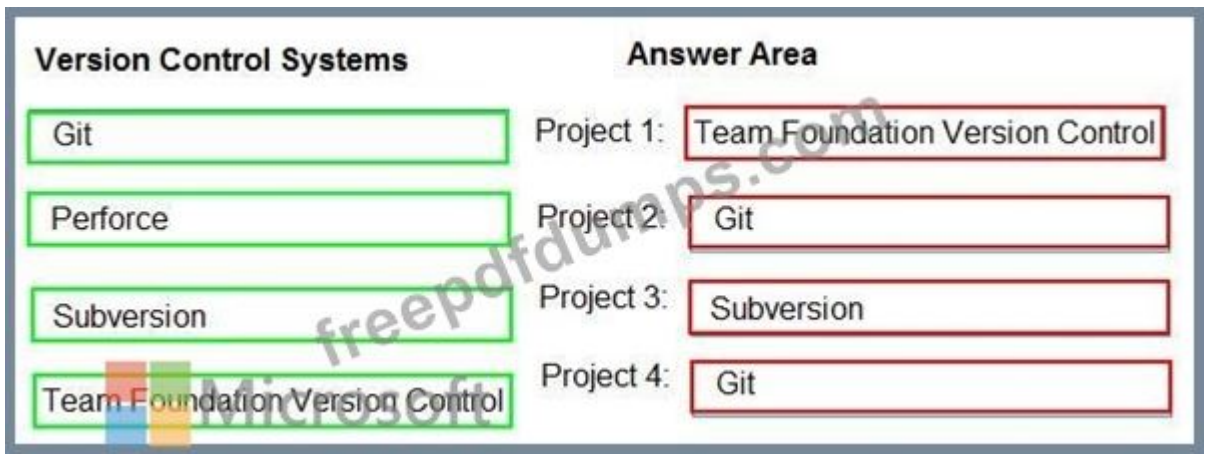
You plan to use Azure Repos for all the projects.

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.



Answer:



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

NEW QUESTION: 132
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: (SHOW ANSWER)
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.

NEW QUESTION: 133
You are developing a multi-tier application. The application will use Azure App Service web apps as the front end and an Azure SQL database as the back end. The application will use Azure functions to write some data to Azure Storage.
You need to send the Azure DevOps team an email message when the front end fails to return a status code of 200.
Which feature should you use?
A. Service Map in Azure Log Analytics
B. Profiler in Azure Application Insights
C. availability tests in Azure Application Insights
D. Application Map in Azure Application Insights
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability

NEW QUESTION: 134
You plane to store signed images in an Azure Container Registry instance named az4009940427acr1.
You need to modify the SKU for az4009940427acr1 to support the planned images. The solution must minimize costs.

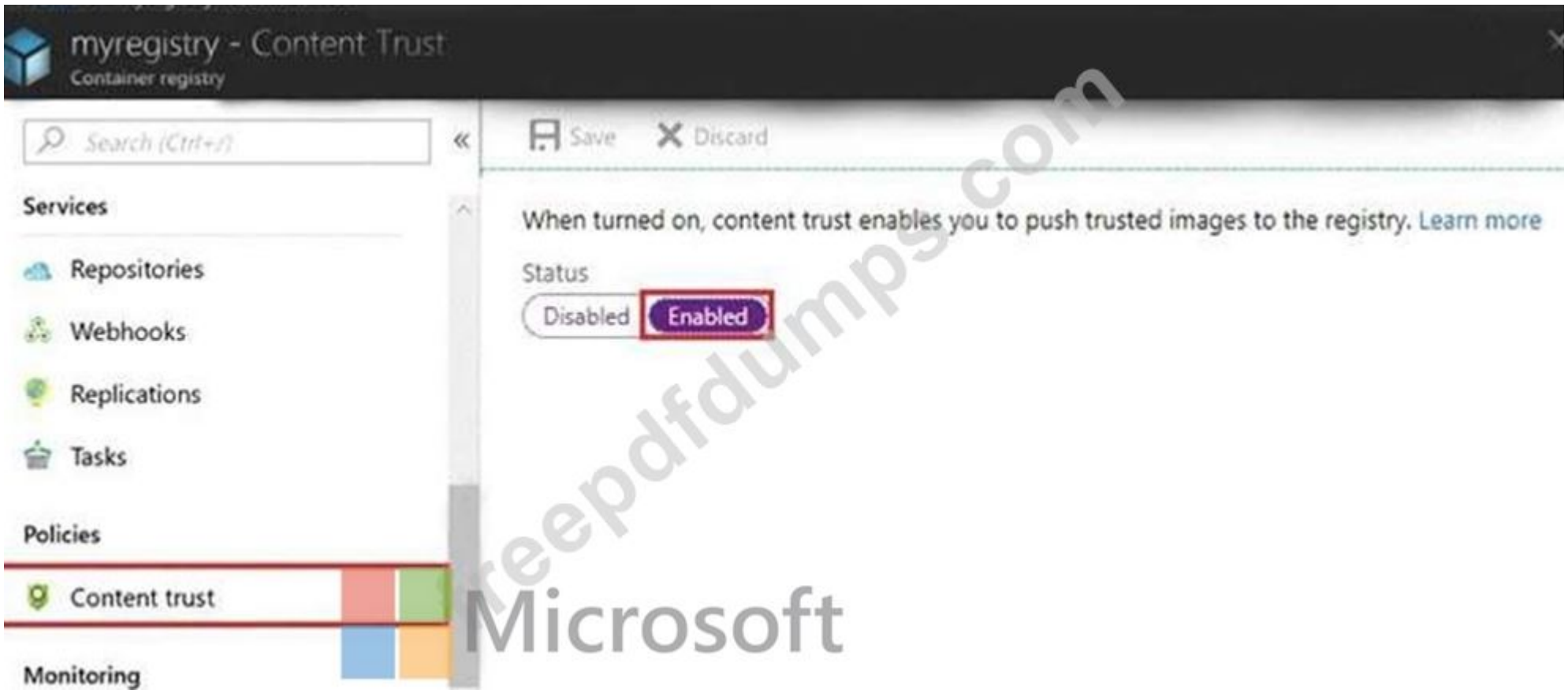
To complete this task, sign in to the Microsoft Azure portal.

Answer:

See solution below.

Explanation

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



References:

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

NEW QUESTION: 135

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-AzureRmAutomationDscNodecmdlet with Register-AzureRmAutomationScheduledRunbook

C. Add the AllowModuleOverwrite parameter.

D. Add the DefaultProfile parameter.

Answer: A (LEAVE A REPLY)

Change the ConfigurationMode parameter from ApplyOnly to ApplyAndAutocorrect.

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

Scenario: Current Technical Issue

The test servers are configured correctly when first deployed, but they experience configuration drift over time.

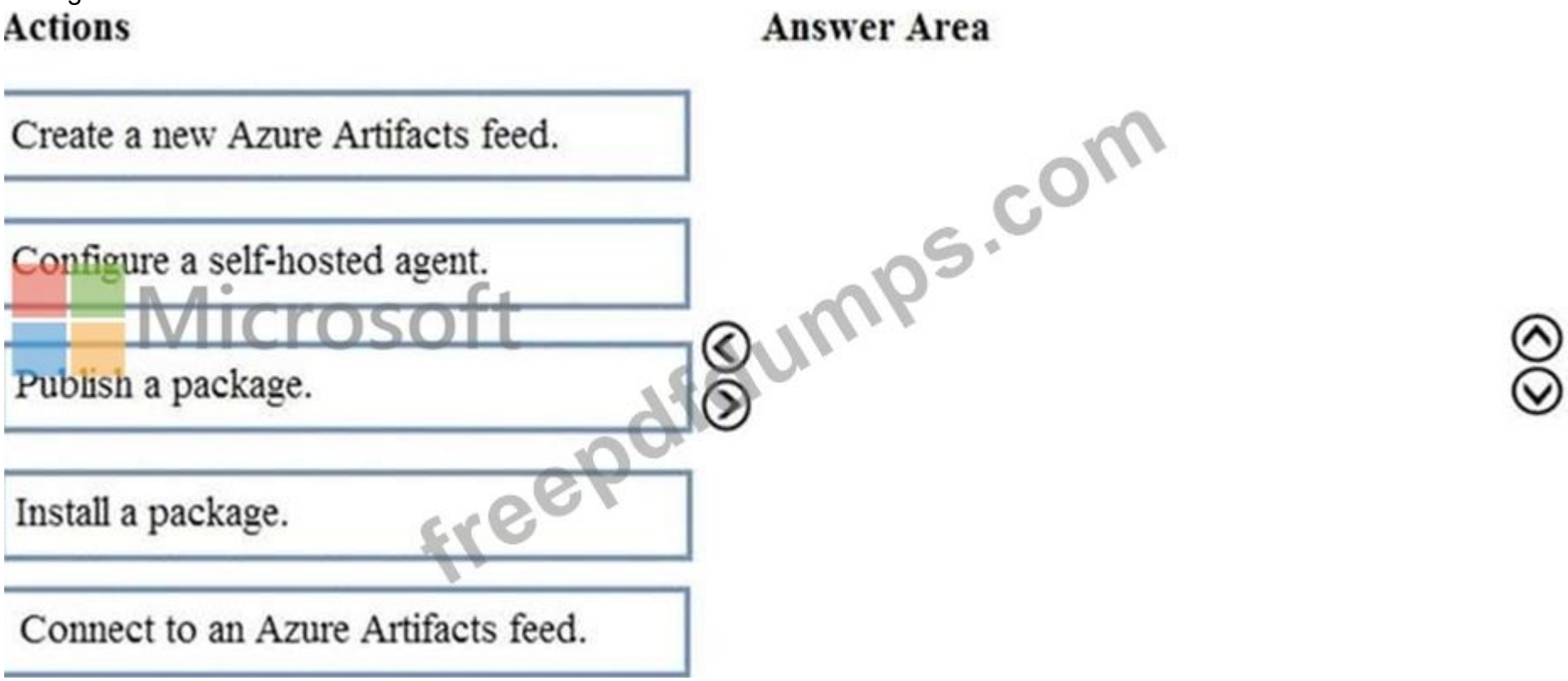
Azure Automation State Configuration fails to correct the configurations.

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

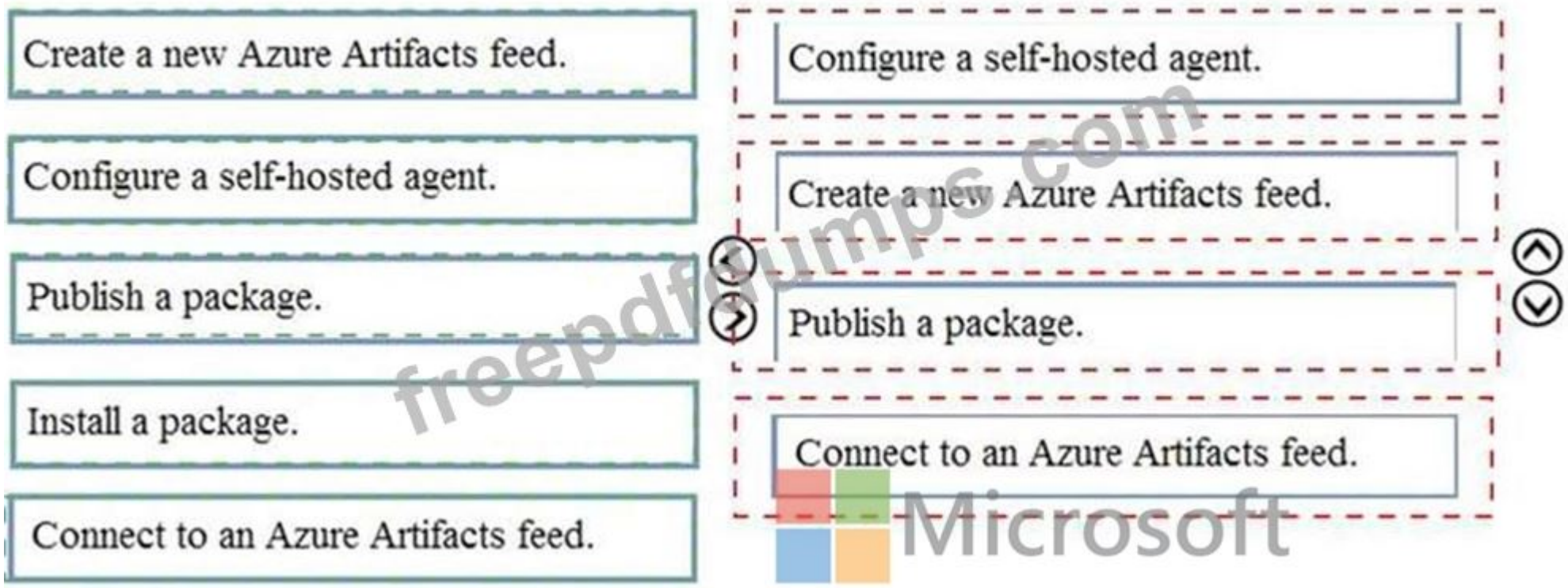
```
Register-AzureRmAutomationDscNode
  -ResourceGroupName 'TestResourceGroup'
  -AutomationAccountName 'LitwareAutomationAccount'
  -AzureVMName $vmanme
  -ConfigurationMode 'ApplyOnly'
```

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

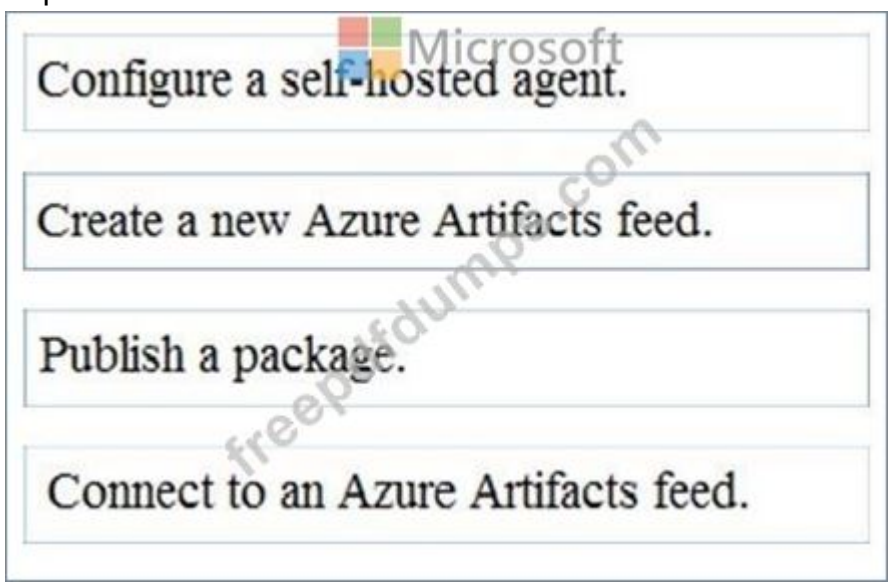
NEW QUESTION: 136
You are creating a NuGet package.
You plan to distribute the package to your development team privately.
You need to share the package and test that the package can be consumed.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation



Step 1: Configure a self-hosted agent.

The build will run on a Microsoft hosted agent.

Step 2: Create a new Azure Artifacts feed

Microsoft offers an official extension for publishing and managing your private NuGet feeds.

Step 3: Publish the package.

Publish, pack and push the built project to your NuGet feed.

Step 4: Connect to an Azure Artifacts feed.

With the package now available, you can point Visual Studio to the feed, and download the newly published package References:

https://medium.com/@dan.cokely/creating-nuget-packages-in-azure-devops-with-azure-pipelines-and-yaml-d6fa

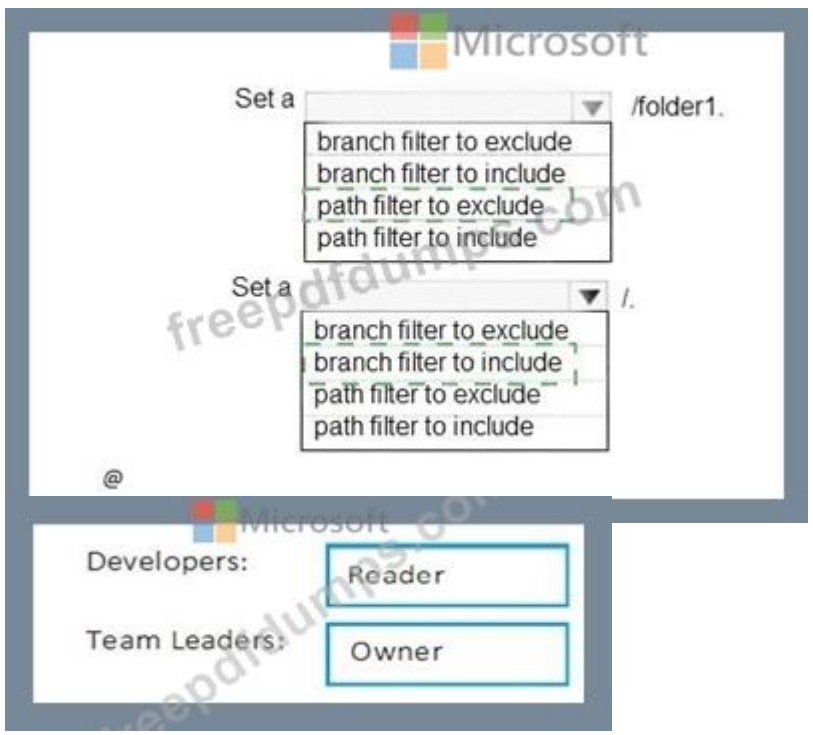
NEW QUESTION: 137

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

Each access level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Answer:



Box 1: Reader

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

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

groups-to any access level.

Box 2: Owner

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

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

NEW QUESTION: 138

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: (SHOW ANSWER)

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

NEW QUESTION: 139

You use Azure DevOps to manage the build and deployment of an app named App1.

You have a 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.

Answer:

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%.

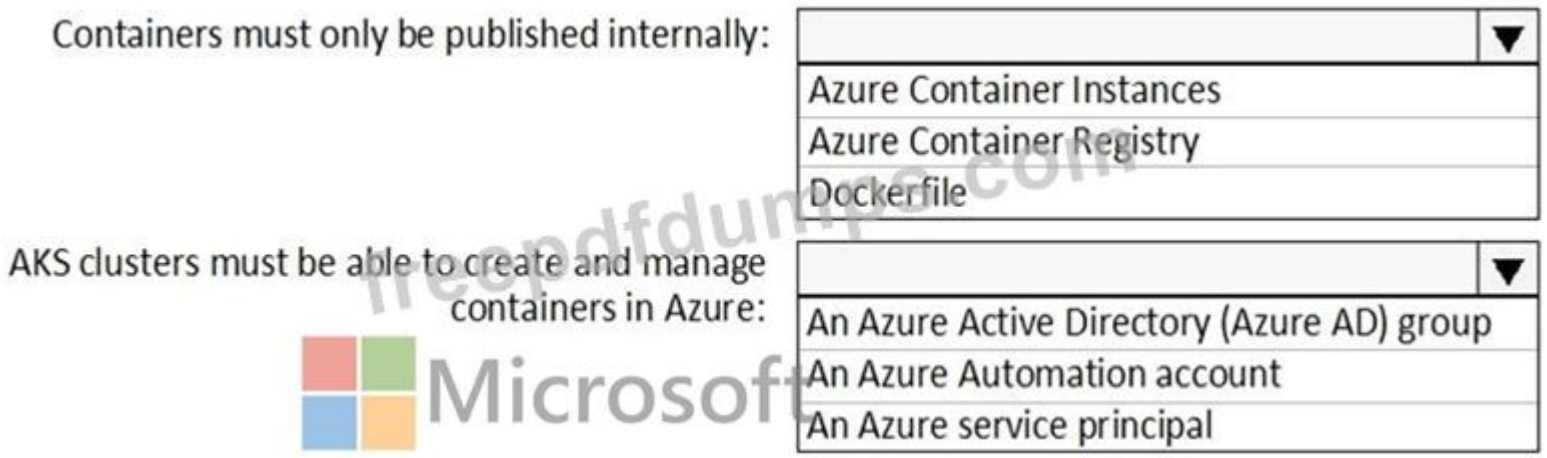
* Aggregation granularity
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric-overview

NEW QUESTION: 140
Your company has an on-premises Bitbucket Server that is used for Git-based source control. The server is protected by a firewall that blocks inbound Internet traffic.
You plan to use Azure DevOps to manage the build and release processes
Which two components are required to integrate Azure DevOps and Bitbucket?
Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one port.
A. an External Git service connection
B. a Microsoft hosted agent
C. service hooks
D. a self- hosted agent
E. a deployment M group
Answer: A,D (LEAVE A REPLY)
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

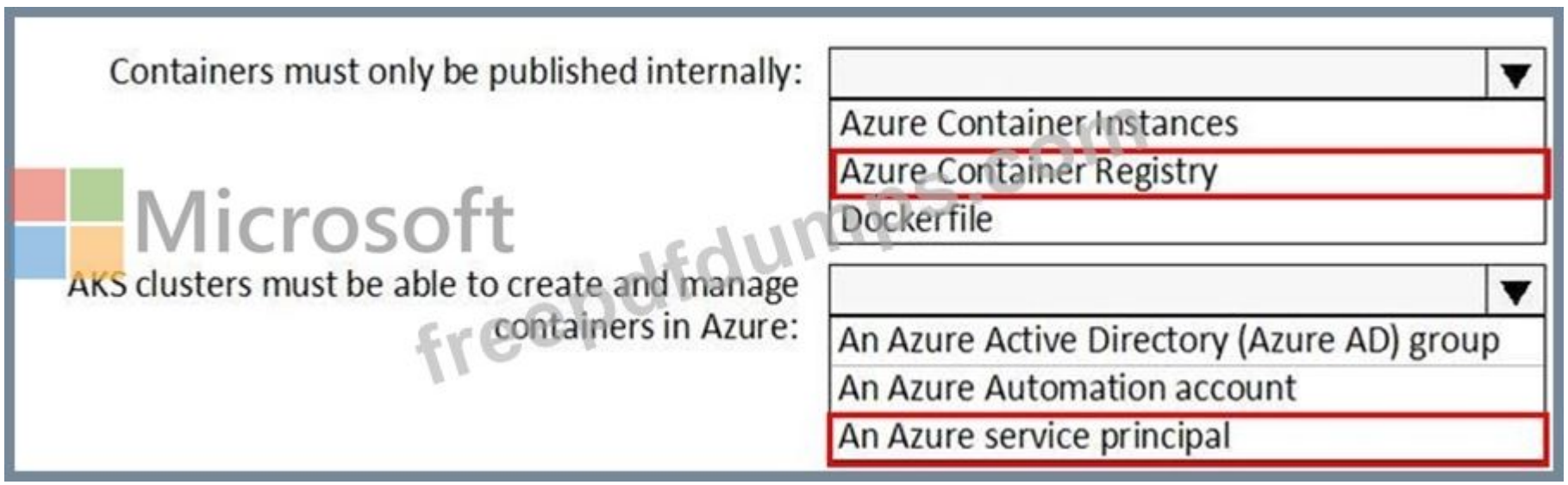
NEW QUESTION: 141
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.
You need to recommend changes to reduce the accumulated technical debt.
Solution: You recommend reducing the code complexity.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
Reference:
https://dzone.com/articles/fight-through-the-pain-how-to-deal-with-technical

NEW QUESTION: 142
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:

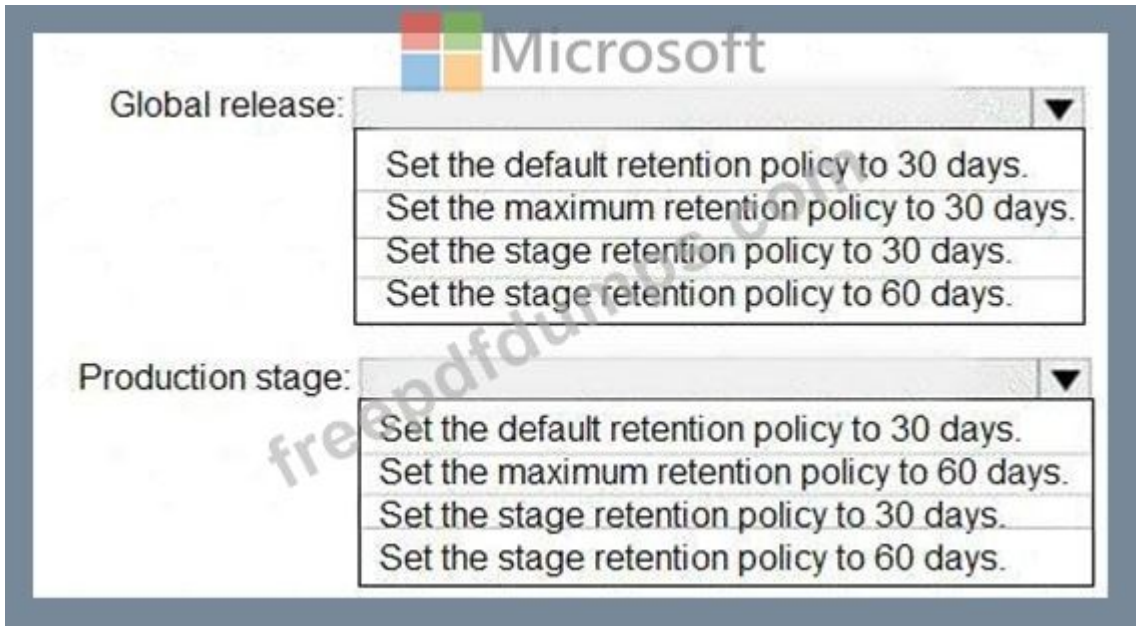


Explanation:
Box 1: Azure Container Registry
Azure services like Azure Container Registry (ACR) and Azure Container Instances (ACI) can be used and connected from independent container orchestrators like kubernetes (k8s). You can set up a custom ACR and connect it to an existing k8s cluster to ensure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

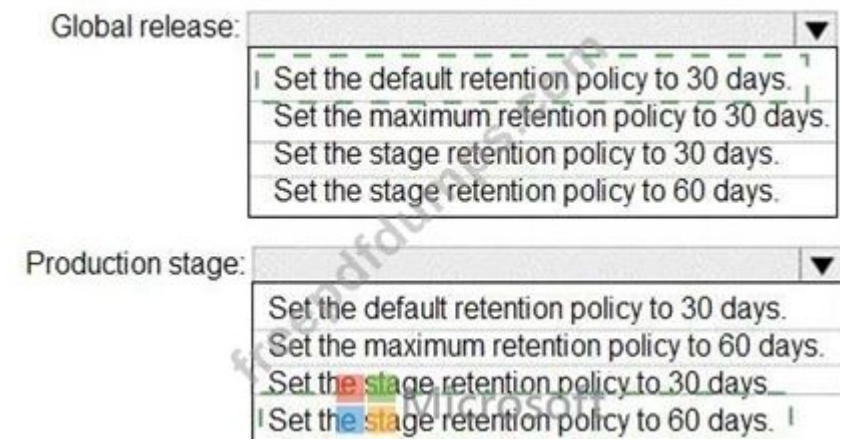
NEW QUESTION: 143
How should you configure the release retention policy for the investment planning applications suite? To answer, select the appropriate options in

the answer area.

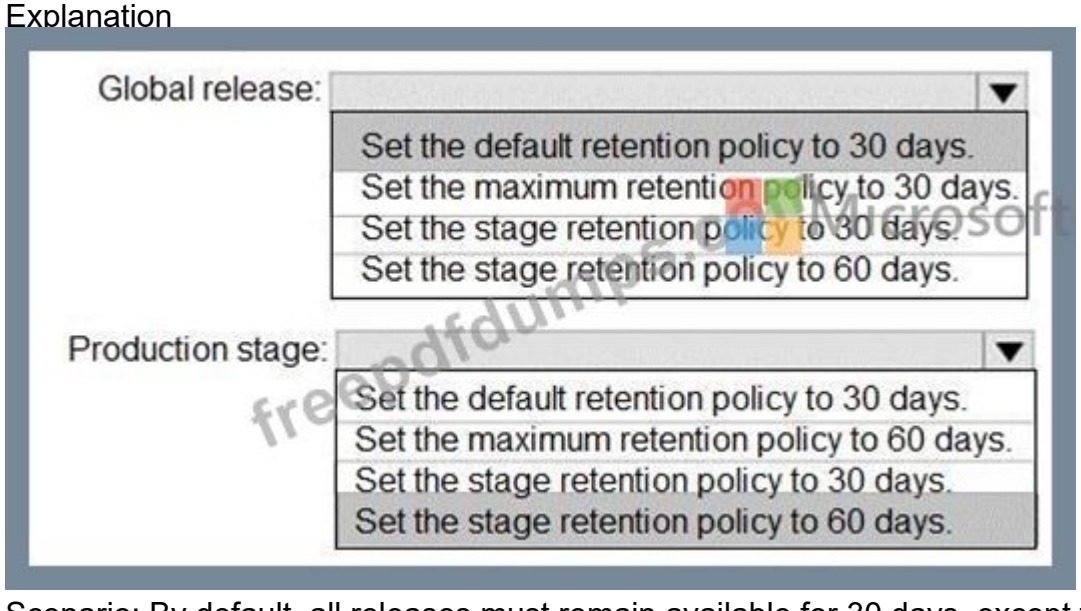
NOTE: Each correct selection is worth one point.



Answer:



Explanation



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

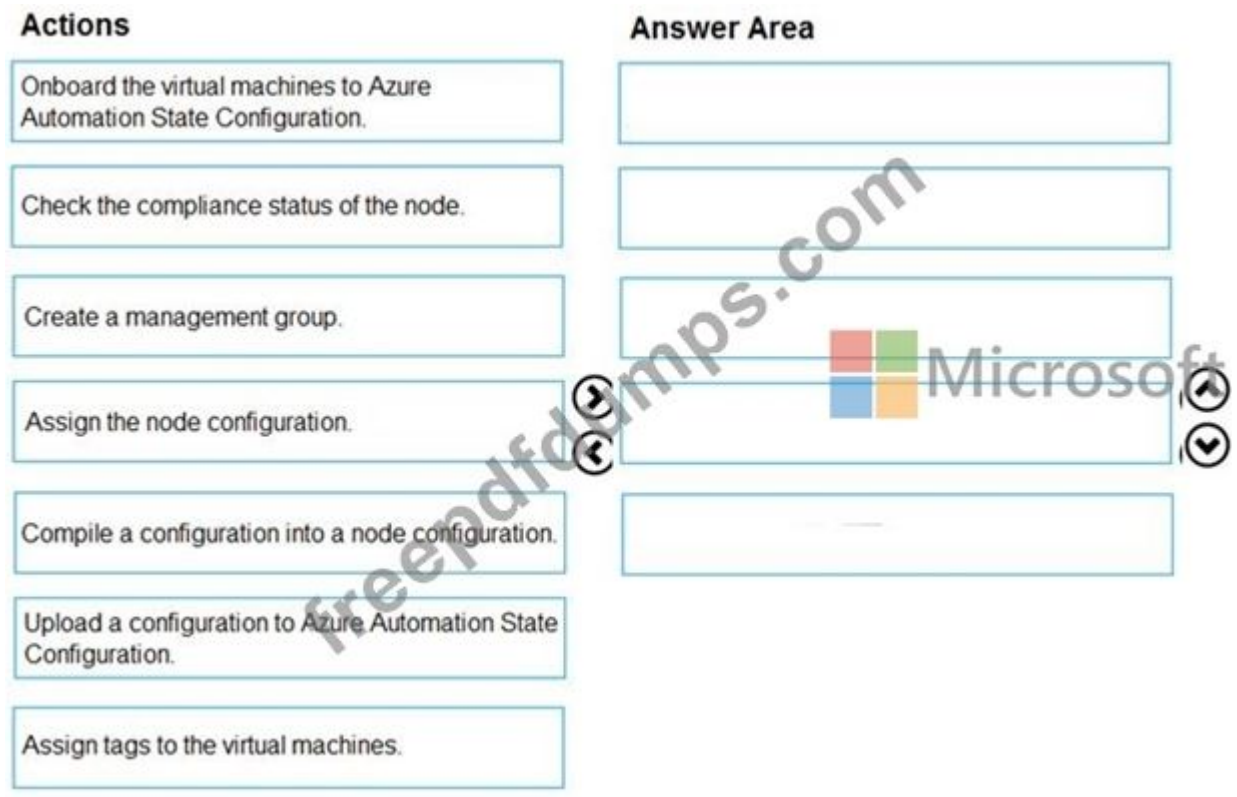
Box 1: Set the default retention policy to 30 days

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

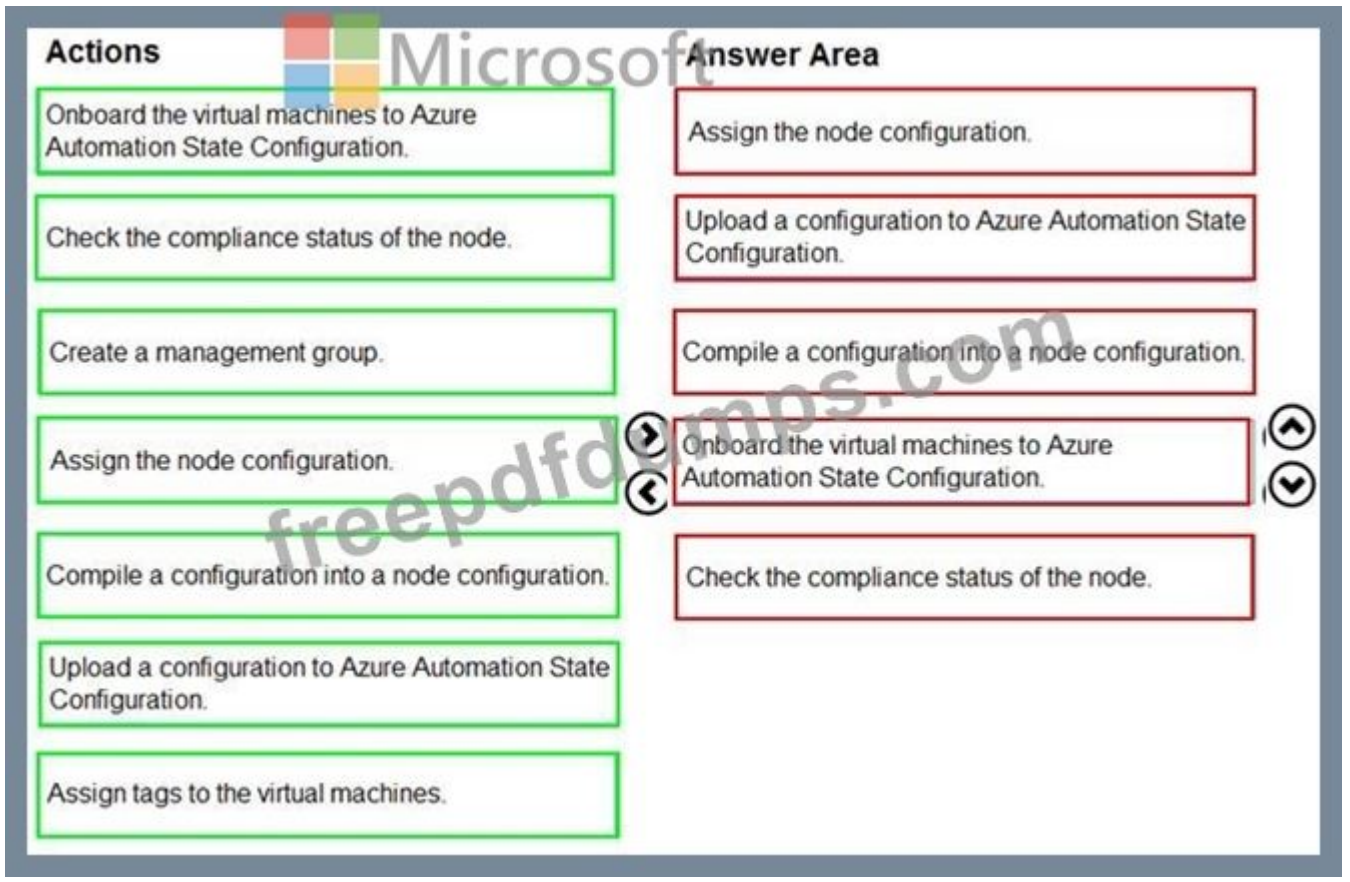
Box 2: Set the stage retention policy to 60 days
You may want to retain more releases that have been deployed to specific stages.
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/policies/retention

NEW QUESTION: 144
Your company creates a web application.
You need to recommend a solution that automatically sends to Microsoft Teams a dairy summary of the exceptions that occur m the application.
Which two Azure services should you recommend? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Microsoft Visual Studio App Center
B. Azure DevOps Project
C. Azure Logic Apps
D. Azure Pipelines
E. Azure Application Insights
Answer: C,E (LEAVE A REPLY)
Explanation
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/asp-net-exceptions
https://docs.microsoft.com/en-us/azure/azure-monitor/app/automate-custom-reports

NEW QUESTION: 145
You need to use Azure Automation Sure Configuration to manage the ongoing consistency of virtual machine configurations.
Which five actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
NOTE: More than one order of answer choices in correct. You writ receive credit for any of the orders you select.



Answer:



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

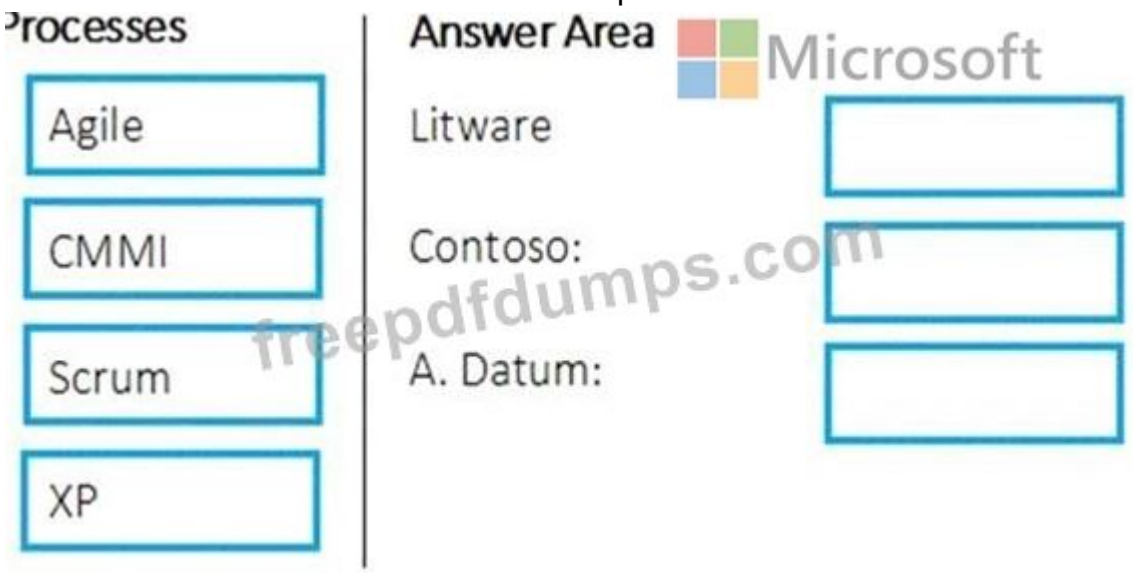
NEW QUESTION: 146
You have an Azure DevOps project named Project1 and an Azure subscription named Sub1. Sub1 contains an Azure SQL database named DB1.
You need to create a release pipeline that uses the Azure SQL Database Deployment task to update DB1.
Which artifact should you deploy?
A. a BACPAC
B. a DACPAC
C. an LDF file
D. an MDF file
Answer: (SHOW ANSWER)
Explanation
Explanation:
Use Azure SQL Database Deployment task in a build or release pipeline to deploy to Azure SQL DB using a DACPAC or run scripts using SQLCMD.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/deploy/sql-azure-dacpac-deployment

NEW QUESTION: 147
You are planning projects for three customers. Each customer's preferred process for work items is shown in the following table.

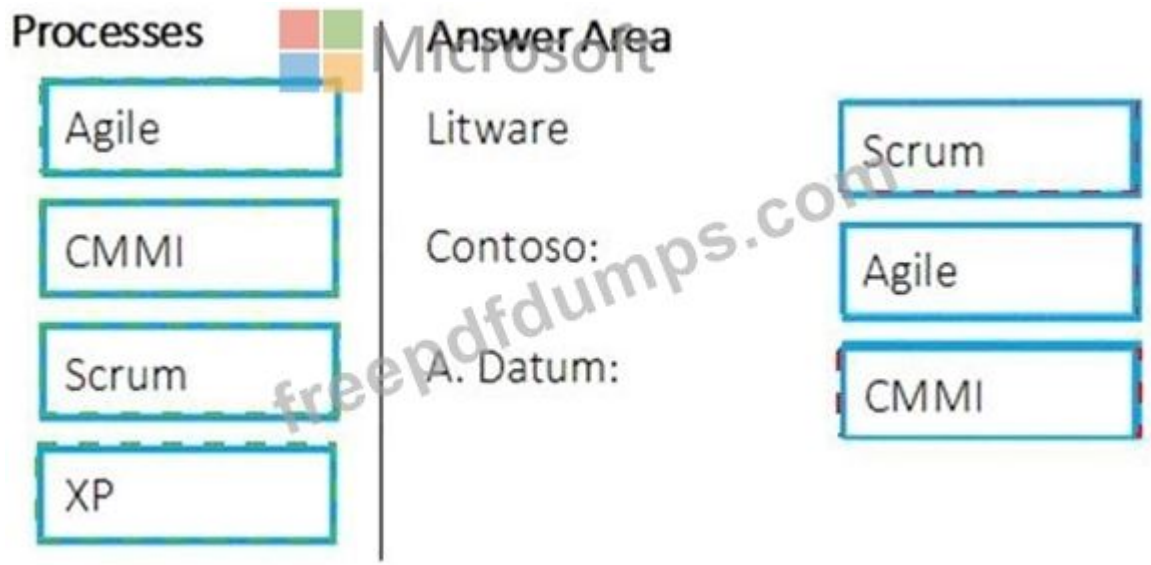
Customer name	Preferred process
Litware, Inc.	Track product backlog items (PBIs) and bugs on the Kanban board. Break the PBIs down into tasks on the task board.
Contoso, Ltd.	Track user stories and bugs on the Kanban board. Track the bugs and tasks on the task board.
A. Datum Corporation	Track requirements,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

The customers all plan to use Azure DevOps for work item management.

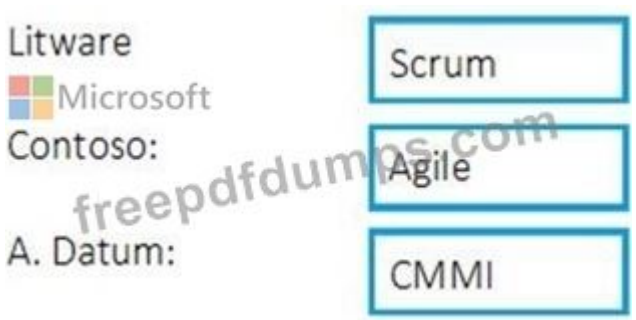
Which work item process should you use for each customer? To answer, drag the appropriate work item process to the correct customers. Each work item process may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:



Explanation



Box 1: Scrum

Choose Scrum when your team practices Scrum. This process works great if you want to track product backlog items (PBIs) and bugs on the Kanban board, or break PBIs and bugs down into tasks on the taskboard.

Box 2: Agile

Choose Agile when your team uses Agile planning methods, including Scrum, and tracks development and test activities separately. This process

works great if you want to track user stories and (optionally) bugs on the Kanban board, or track bugs and tasks on the taskboard.
Box 3: CMMI
Choose CMMI when your team follows more formal project methods that require a framework for process improvement and an auditable record of decisions. With this process, you can track requirements, change requests, risks, and reviews.

NEW QUESTION: 148
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: A (LEAVE A REPLY)
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/

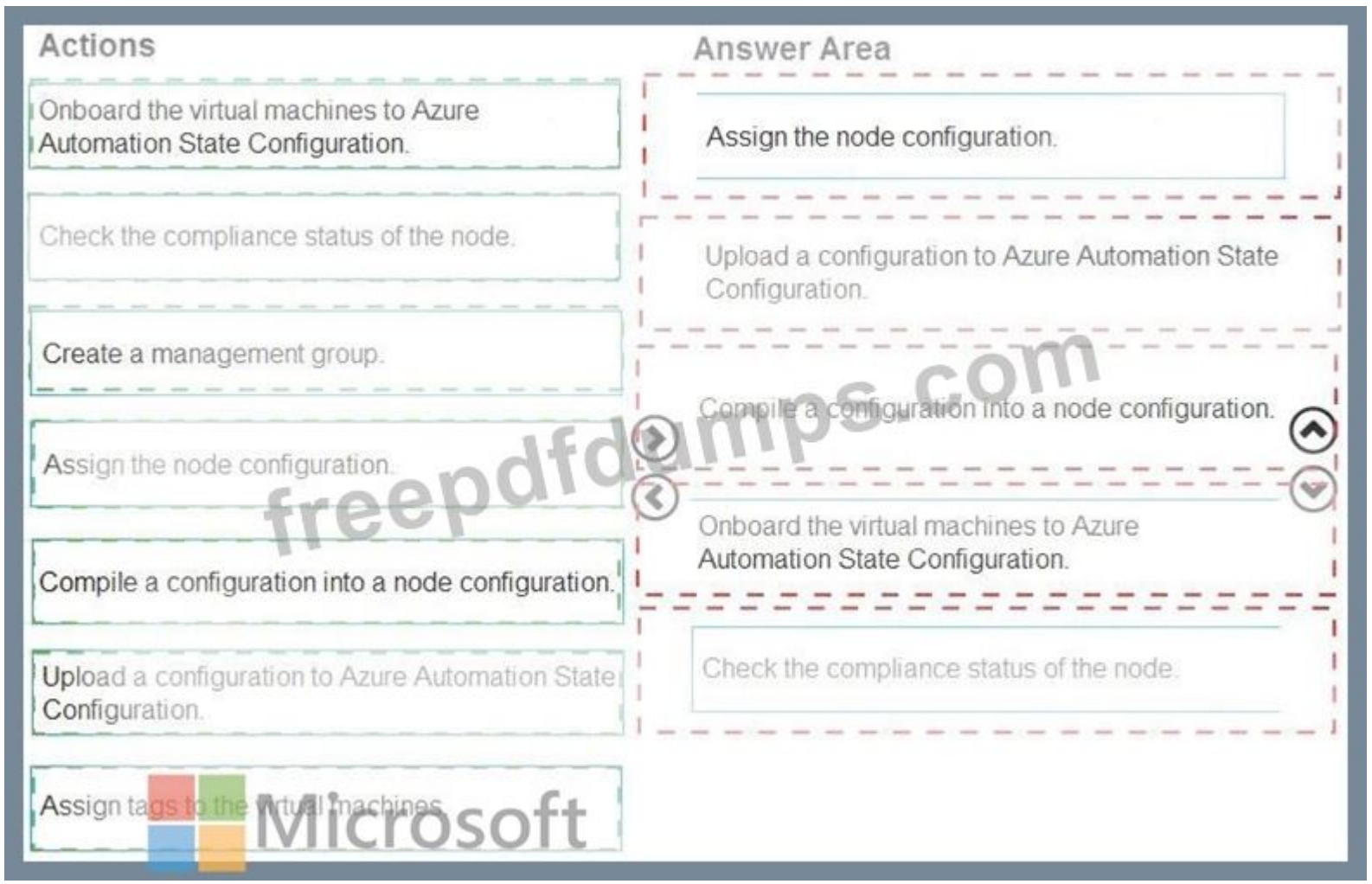
NEW QUESTION: 149
You have an Azure DevOps organization named Contoso.
You need to receive Microsoft Teams notifications when work items are updated.
What should you do?
A. From Azure DevOps. configure a service hook subscription.
B. From Microsoft Teams, configure a connector.
C. From Microsoft Teams, add a channel.
D. From Azure DevOps. install an extension.
E. From the Microsoft Teams admin center configure external access.
Answer: A (LEAVE A REPLY)
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

NEW QUESTION: 150

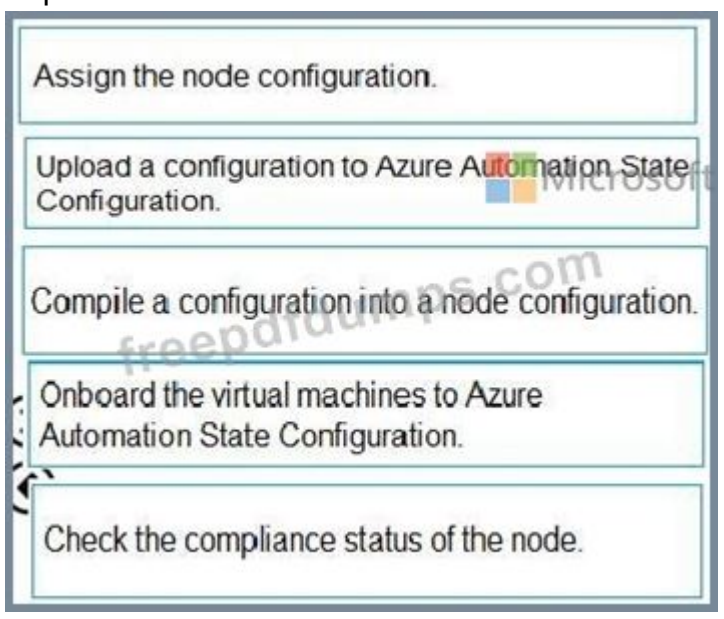
You need to use Azure Automation Sure Configuration to manage the ongoing consistency of virtual machine configurations.

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

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



Explanation



Step 1: Assign the node configuration.

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

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

You import the configuration into the Automation account.

Step 3: Compiling a configuration into a node configuration

Compiling a configuration in Azure Automation
Before you can apply a desired state to a node, a DSC configuration defining that state must be compiled into one or more node configurations (MOF document), and placed on the Automation DSC Pull Server.
Step 4: Onboard the virtual machines to Azure State Configuration
Onboarding an Azure VM for management with Azure Automation State Configuration Step 5: Check the compliance status of the node.
Viewing reports for managed nodes. Each time Azure Automation State Configuration performs a consistency check on a managed node, the node sends a status report back to the pull server. You can view these reports on the page for that node.
On the blade for an individual report, you can see the following status information for the corresponding consistency check:
The report status - whether the node is "Compliant", the configuration "Failed", or the node is "Not Compliant" (when the node is in ApplyandMonitor mode and the machine is not in the desired state).
References: https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

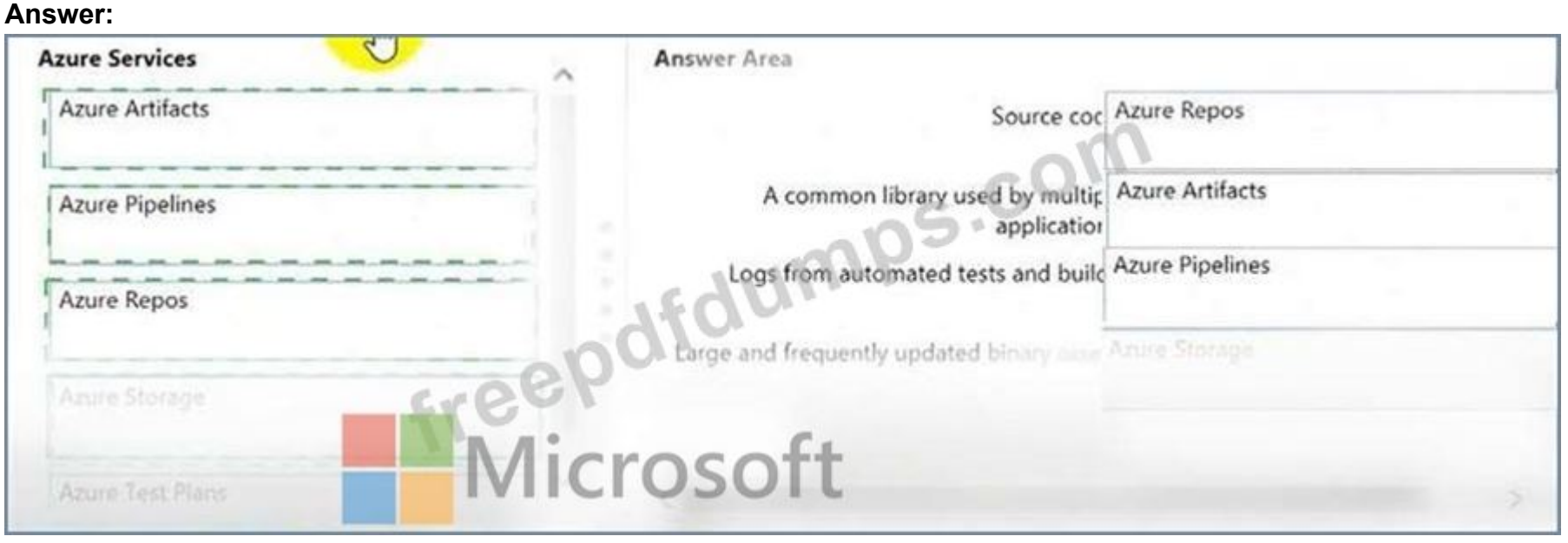
NEW QUESTION: 151
You use Azure Pipelines to manage project builds and deployments.
You plan to use Azure Pipelines for Microsoft Teams to notify the legal team when a new build is ready for release. You need to configure the Organization Settings in Azure DevOps to support Azure Pipelines for Microsoft Teams. What should you turn on?
A. Azure Active Directory Conditional Access Policy Validation
B. Alternate authentication credentials
C. SSH authentication
D. Third-party application access via OAuth
Answer: D (LEAVE A REPLY)

NEW QUESTION: 152
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 (LEAVE A REPLY)
Explanation
Use Azure SQL Database Deployment task in a build or release pipeline to deploy to Azure SQL DB using a DACPAC or run scripts using SQLCMD.

Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/deploy/sql-azure-dacpac-deployment

NEW QUESTION: 153
Your company is building a new web application.
You plan to collect feedback from pilot users on the features being delivered.
All the pilot users have a corporate computer that has Google Chrome and the Microsoft Test & Feedback extension installed. The pilot users will test the application by using Chrome.
You need to identify which access levels are required to ensure that developers can request and gather feedback from the pilot users. The solution must use the principle of least privilege.
Which access levels m Azure DevOps should you identify? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Answer:

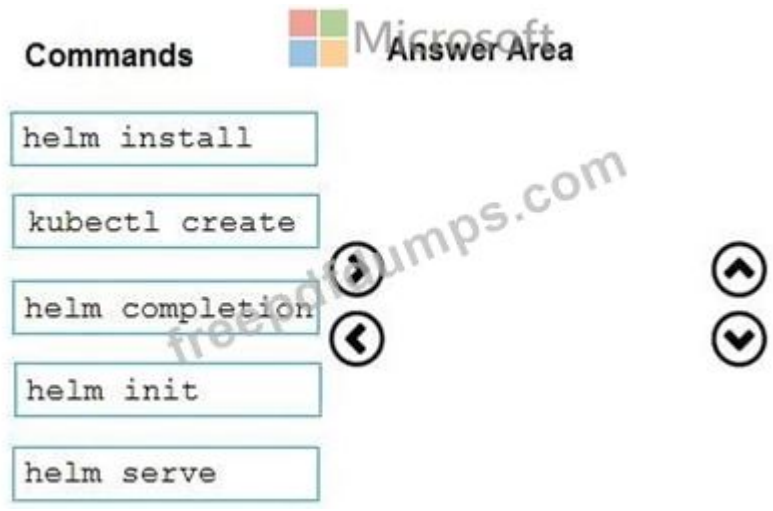


Explanation

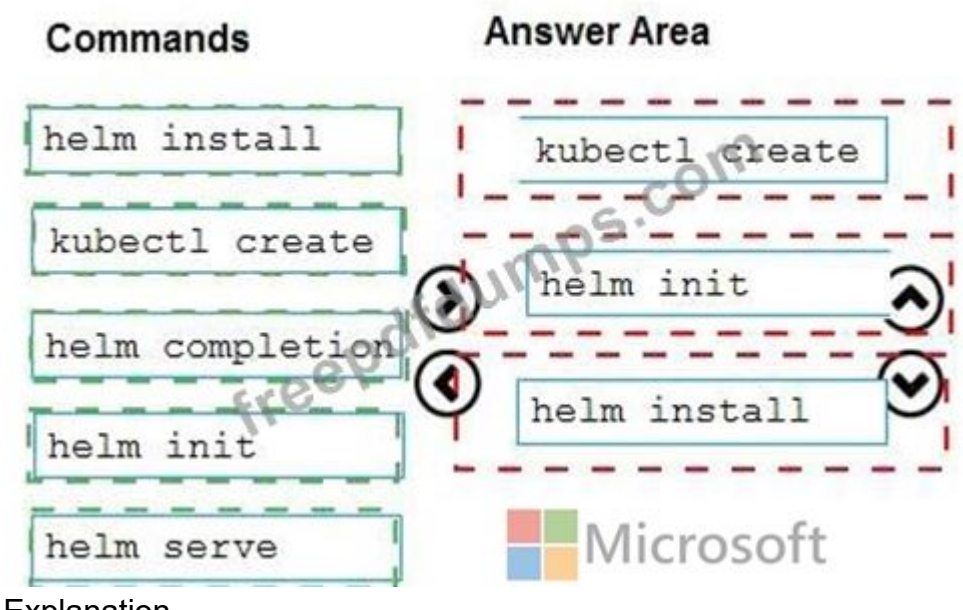
Box 1: Basic
Assign Basic to users with a TFS CAL, with a Visual Studio Professional subscription, and to users for whom you are paying for Azure Boards &

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

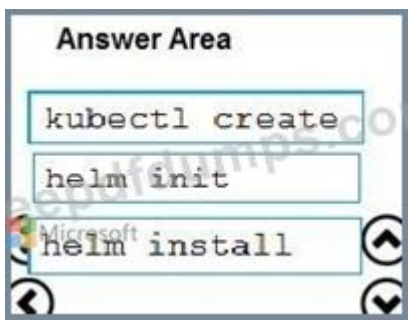
NEW QUESTION: 154
You need to recommend a solution for deploying charts by using Helm and Title to Azure Kubemets Service (AKS) in an RBAC-enabled cluster.
Which three commands should you recommend be run m sequence? To answer, move the appropriate commands from the list of commands to the answer area and arrange them in the correct order.



Answer:



Explanation



Step 1: Kubectl create

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

Example: Service account with cluster-admin role

$ kubectl create -f rbac-config.yaml

serviceaccount "tiller" created

clusterrolebinding "tiller" created

$ helm init --service-account tiller

Step 2: helm init

To deploy a basic Tiller into an AKS cluster, use the helm init command.

Step 3: helm install

To install charts with Helm, use the helm install command and specify the name of the chart to install.

References:

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

https://docs.helm.sh/using_helm/#tiller-namespaces-and-rbac

NEW QUESTION: 155

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:

Explanation

Box 1: Azure Pipelines service connection

Box 2: Managed Service Identity Authentication

The managed identities for Azure resources feature in Azure Active Directory (Azure AD) provides Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code.

Reference:

https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/deploy/azure-key-vault

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

NEW QUESTION: 156

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

What should you include in the solution? To answer, select the appropriate options m the answer atea, NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Every request made against a storage service must be authorized, unless the request is for a blob or container resource that has been made available for public or signed access. One option for authorizing a request is by using Shared Key.

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

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

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

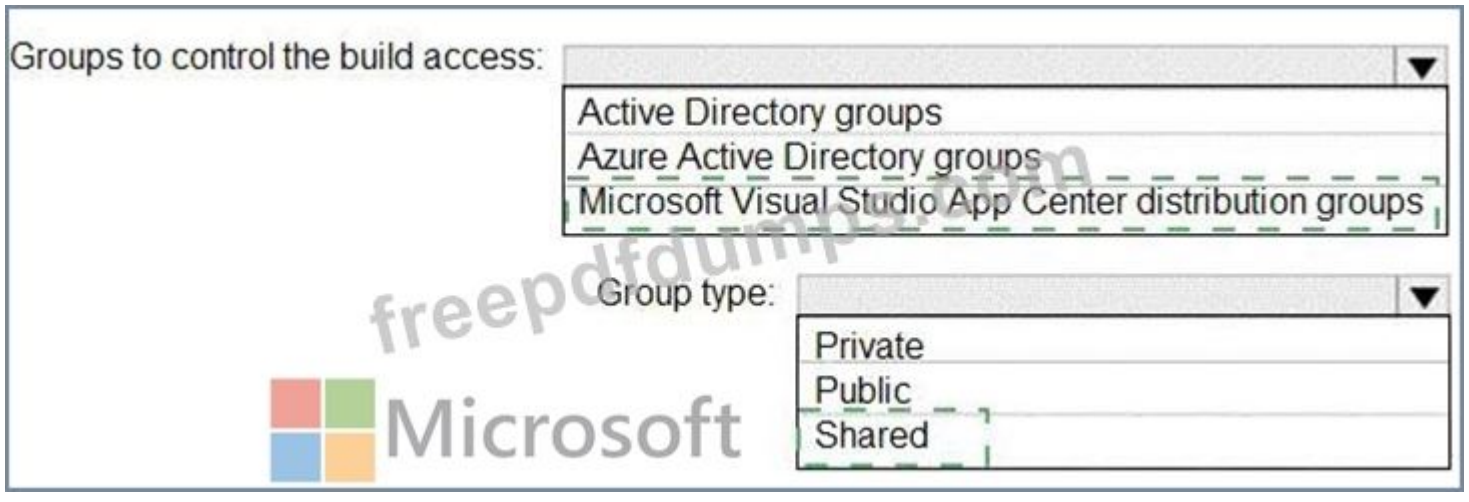
NEW QUESTION: 157

Your company is creating a suite of three mobile applications.

You need to control access to the application builds. The solution must be managed at the organization level What should you use? To answer, select the appropriate options m the answer area.

NOTE: Each correct selection is worth one point.

Answer:



Explanation

Box 1: Microsoft Visual Studio App Center distribution Groups

Distribution Groups are used to control access to releases. A Distribution Group represents a set of users that can be managed jointly and can have common access to releases. Example of Distribution Groups can be teams of users, like the QA Team or External Beta Testers or can represent stages or rings of releases, such as Staging.

Box 2: Shared

Shared distribution groups are private or public distribution groups that are shared across multiple apps in a single organization. Shared distribution groups eliminate the need to replicate distribution groups across multiple apps.

Note: With the Deploy with App Center Task in Visual Studio Team Services, you can deploy your apps from Azure DevOps (formerly known as VSTS) to App Center. By deploying to App Center, you will be able to distribute your builds to your users.

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

NEW QUESTION: 158

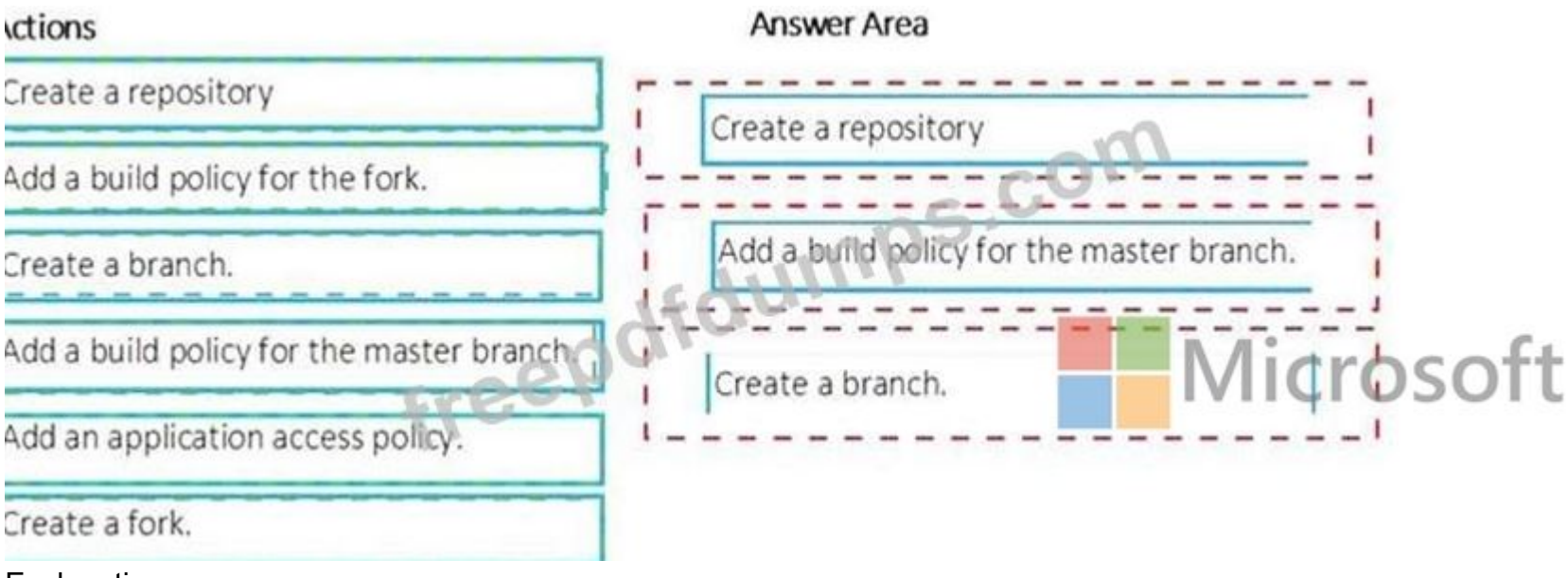
You have an Azure subscription that contains a resources group named RG1. RG1 contains the following resources:

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

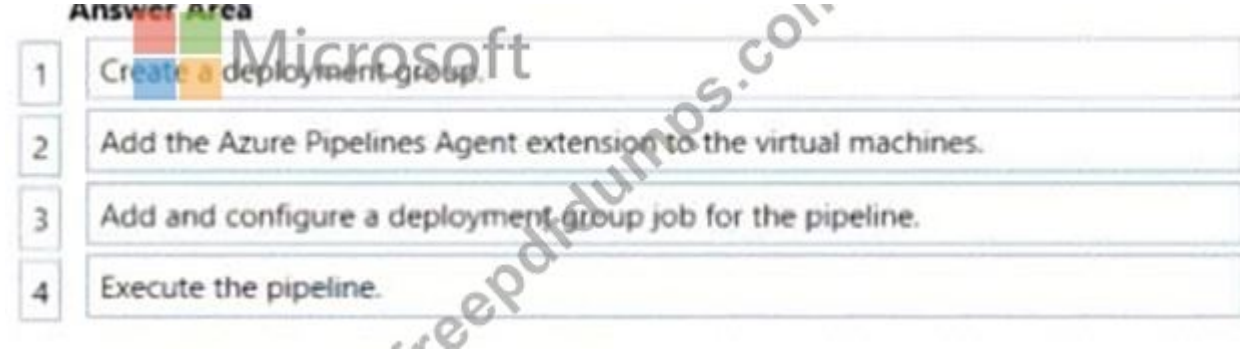
You need to deploy an application to the virtual machines in RG1 by using Azure Pipelines.

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.

Answer:



Explanation



NEW QUESTION: 159

Your company has an on-premises Bitbucket Server that is used for Git-based source control. The server is protected by a firewall that blocks inbound Internet traffic.

You plan to use Azure DevOps to manage the build and release processes.

Which two components are required to integrate Azure DevOps and Bitbucket? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a deployment group

B. a Microsoft-hosted agent

C. service hooks

D. a self-hosted agent

E. an External Git service connection

Answer: (SHOW ANSWER)

Explanation/Reference:
Explanation:
E: GitLab CI/CD can be used with GitHub or any other Git server such as BitBucket. Instead of moving your entire project to GitLab, you can connect your external repository to get the benefits of GitLab CI/CD.
Note: 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-git Testlet 1 Case Study This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
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

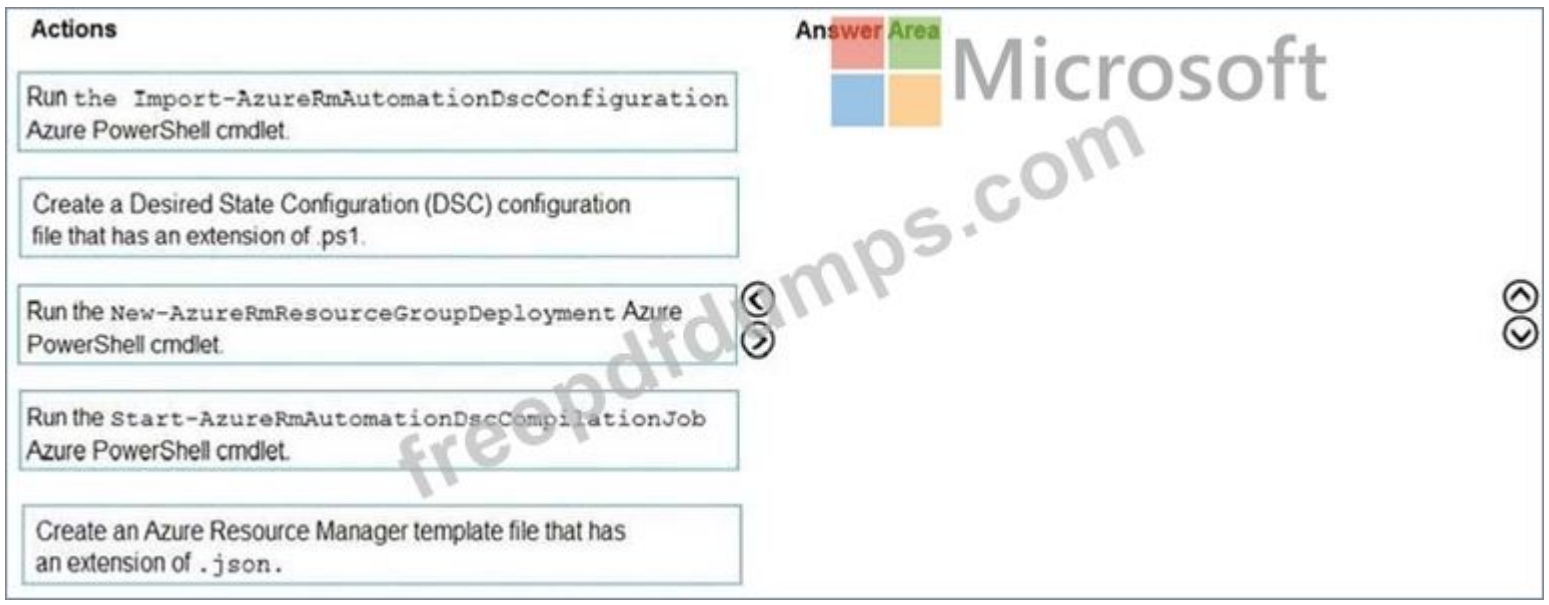
be used by employees; the other will be used by customers.
Litware plans to move to a more agile development methodology. Shared code will be extracted into a series of packages.
Litware has started an internal cloud transformation process and plans to use cloud-based services whenever suitable.
Litware 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.

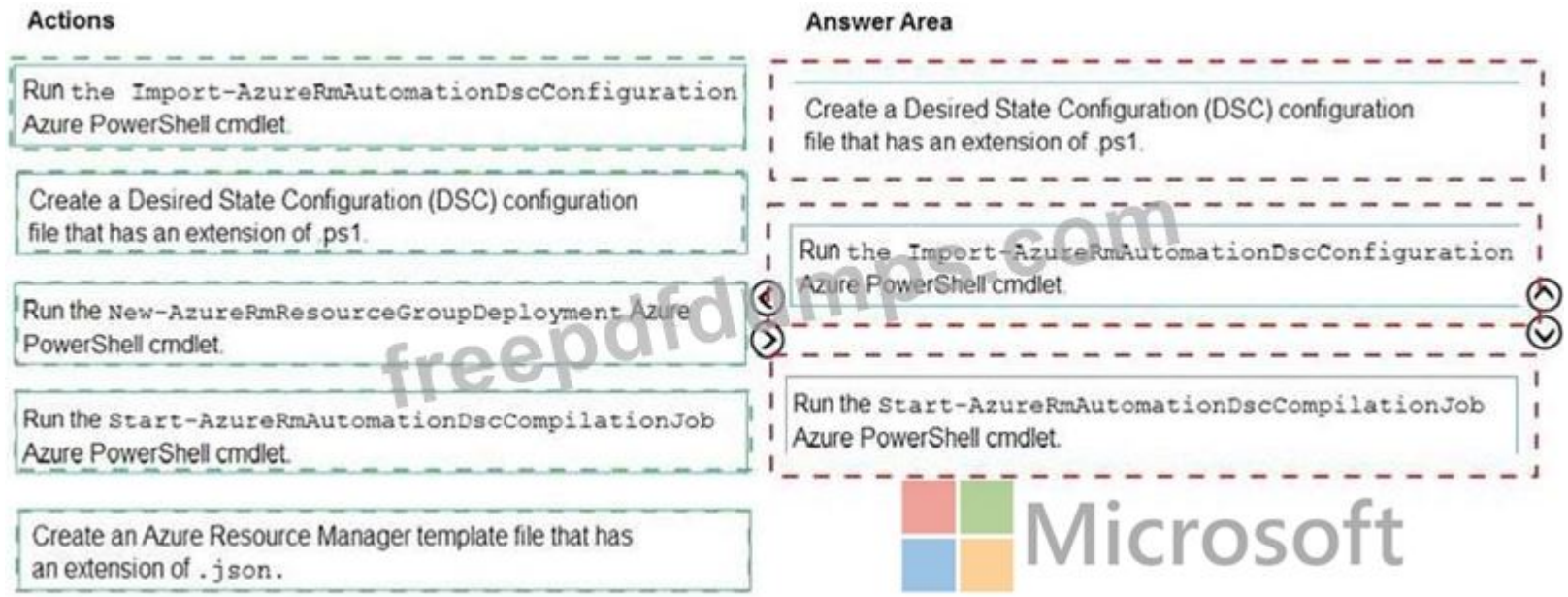
Current Technical Issue
The test servers are configured correctly when first deployed, but they experience configuration drift over time. Azure Automation State Configuration fails to correct the configurations.
Azure Automation State Configuration nodes are registered by using the following command.

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

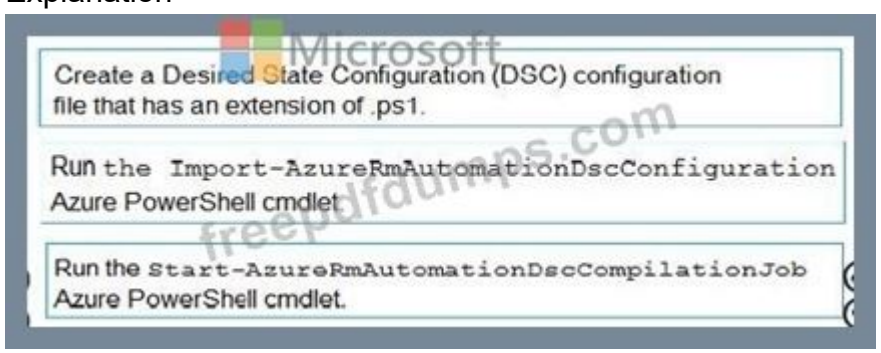
NEW QUESTION: 160
You need to configure Azure Automation for the computer in Group7.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation



Step 1: Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1.

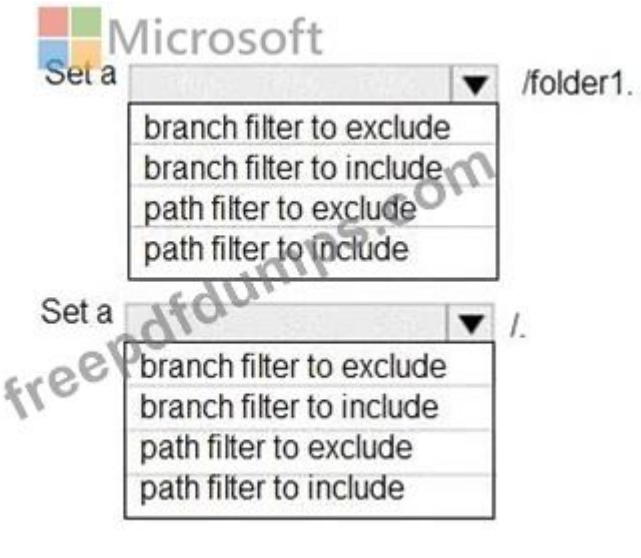
Step 2: Run the Import-AzureRmAutomationDscConfiguration Azure Powershell cmdlet The Import-AzureRmAutomationDscConfiguration cmdlet imports an APS Desired State Configuration (DSC) configuration into Azure Automation. Specify the path of an APS script that contains a single DSC configuration.

Example:

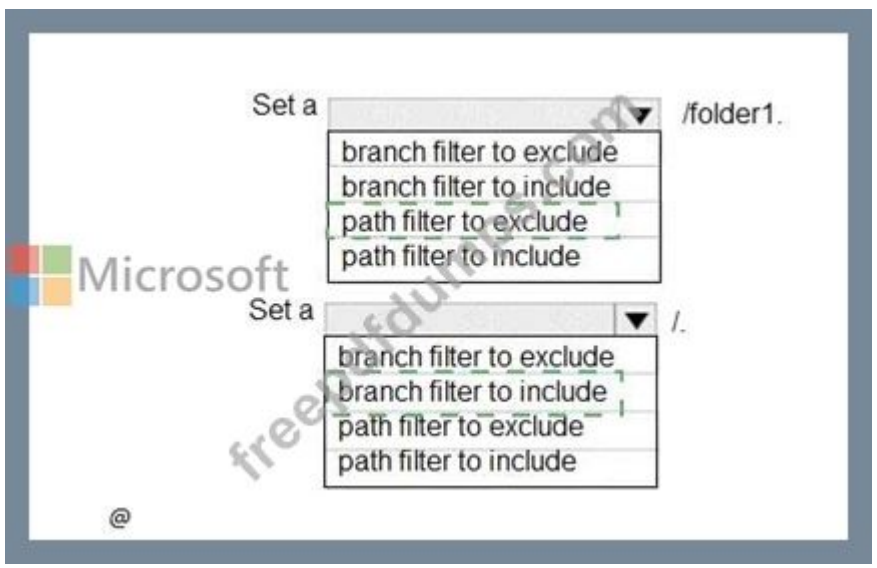
PS C:\>Import-AzureRmAutomationDscConfiguration -AutomationAccountName "Contoso17"-ResourceGroupName "ResourceGroup01" -SourcePath "C:\DSC\client.ps1" -Force This command imports the DSC configuration in

the file named client.ps1 into the Automation account named Contoso17. The command specifies the Force parameter. If there is an existing DSC configuration, this command replaces it.
Step 3: Run the Start-AzureRmAutomationDscCompilationJob Azure Powershell cmdlet The Start-AzureRmAutomationDscCompilationJob cmdlet compiles an APS Desired State Configuration (DSC) configuration in Azure Automation.
References:
https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/import-azurermautomationdscconfigur
https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/start-azurermautomationdsccompilatio

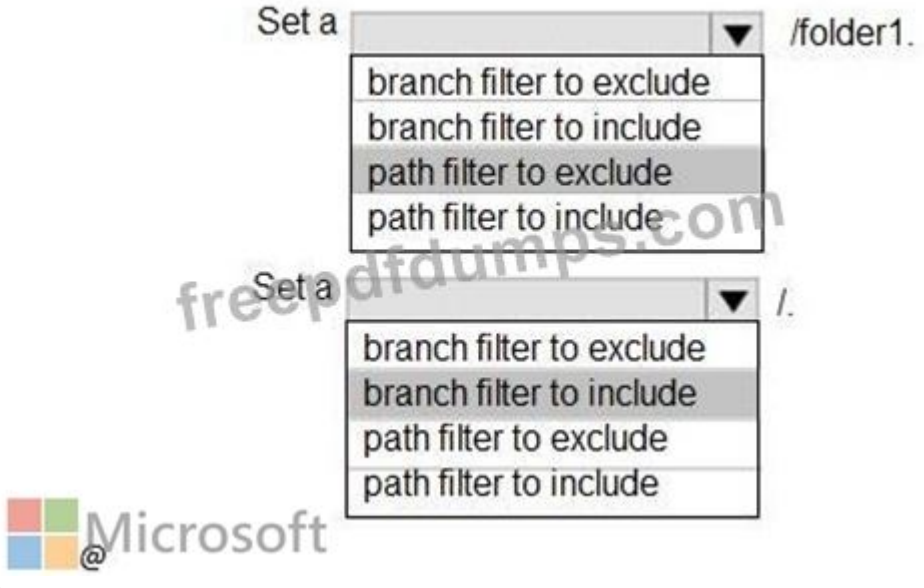
NEW QUESTION: 161
How should you configure the filters for the Project5 trigger? To answer, select the appropriate option in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation



Scenario:

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

Topic 2, Case Study: 1Overview

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.NE T web forms that use logic written in V8.NET. Some new sections of the application are written in C#.

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

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

Architectural Issues

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

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

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

Requirements

Planned Changes

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

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

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

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

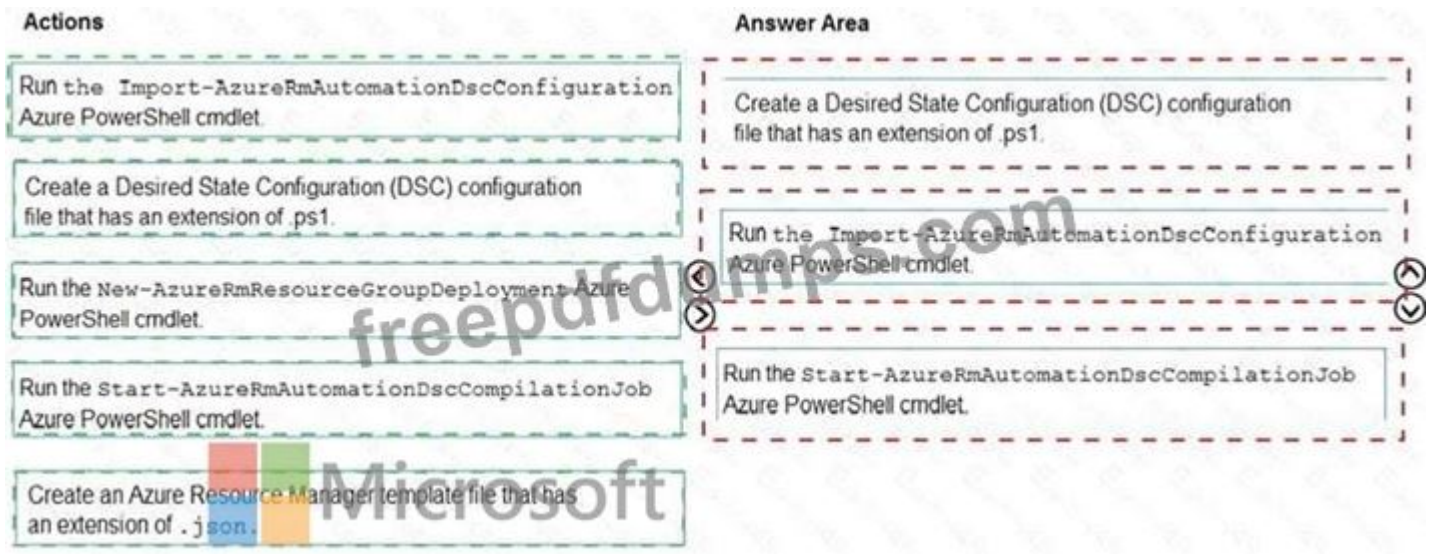
Litware wants to become proactive m detecting failures, rather than always waning for customer bug reports.

Technical Requirements
The company's investment planning applications suite must meet the following technical requirements:
* New incoming connections through the firewall must be minimized.
* Members of a group named Developers must be able to install packages.
* The principle of least privilege must be used for all permission assignments
* A branching strategy that supports developing new functionality in isolation must be used.
* Members of a group named Team leaders must be able to create new packages and edit the permissions of package feeds
* Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use.
* By default, all App Center must be used to centralize the reporting of mobile application crashes and device types in use.
* Code quality and release quality are critical. During release, deployments must not proceed between stages if any active bugs are logged against the release.
* The mobile applications must be able to call the share pricing service of the existing retirement fund management system. Until the system is upgraded, the service will only support basic authentication over HUPS.
* The required operating system configuration tor the test servers changes weekly. Azure Automation State Configuration must be used to ensure that the operating system on each test servers configured the same way when the servers are created and checked periodically.
Current Technical
The test servers are configured correctly when first deployed, but they experience configuration drift over time. Azure Automation State Configuration fails to correct the configurations.
Azure Automation State Configuration nodes are registered by using the following command.

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

NEW QUESTION: 162
How should you confrere the release retention policy for the investment planning depletions suite? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:



Explanation

Every request made against a storage service must be authorized, unless the request is for a blob or container resource that has been made available for public or signed access. One option for authorizing a request is by using Shared Key.

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

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

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

NEW QUESTION: 163

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: B,D (LEAVE A REPLY)

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

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

Reference:

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

NEW QUESTION: 164

You are implementing an Azure DevOps strategy for mobile devices using App Center.

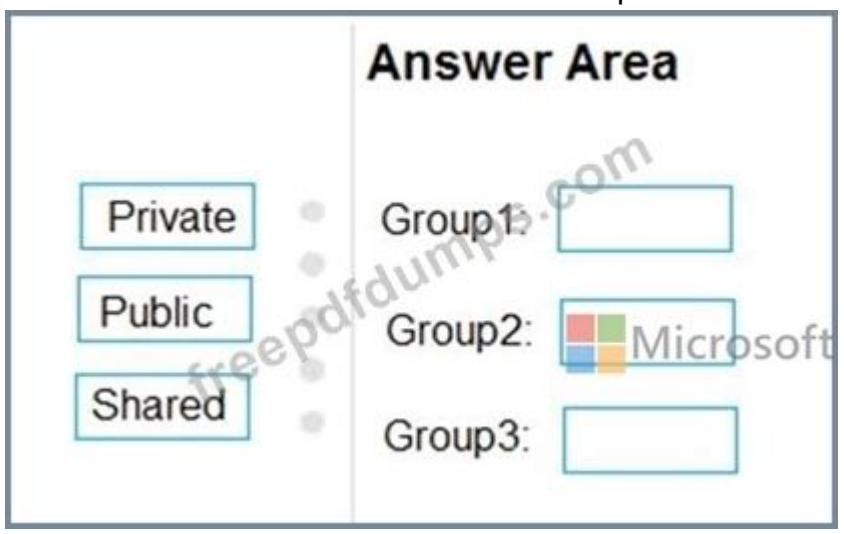
You plan to use distribution groups to control access to releases.

You need to create the distribution groups shown in the following table.

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

Which type of distribution group should you use for each group? To answer, drag the appropriate group types to the correct locations. Each group type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Box1: Private

In App Center, distribution groups are private by default. Only testers invited via email can access the releases available to this group.

Box 2: Public

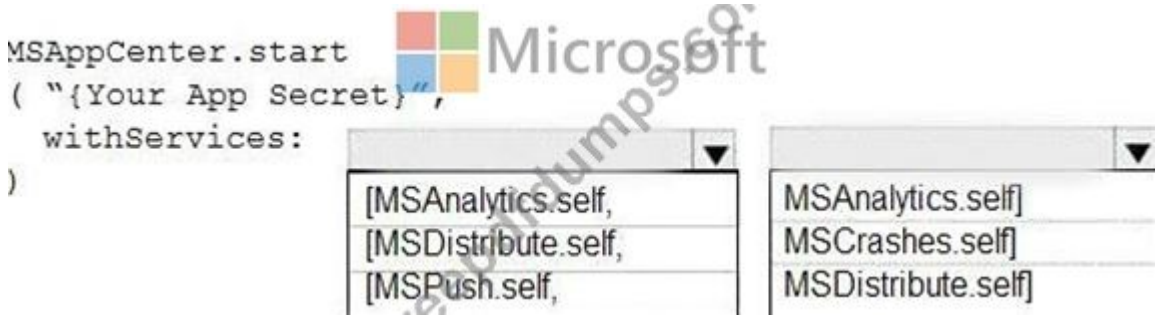
Distribution groups must be public to enable unauthenticated installs from public links.

Box 3: Shared

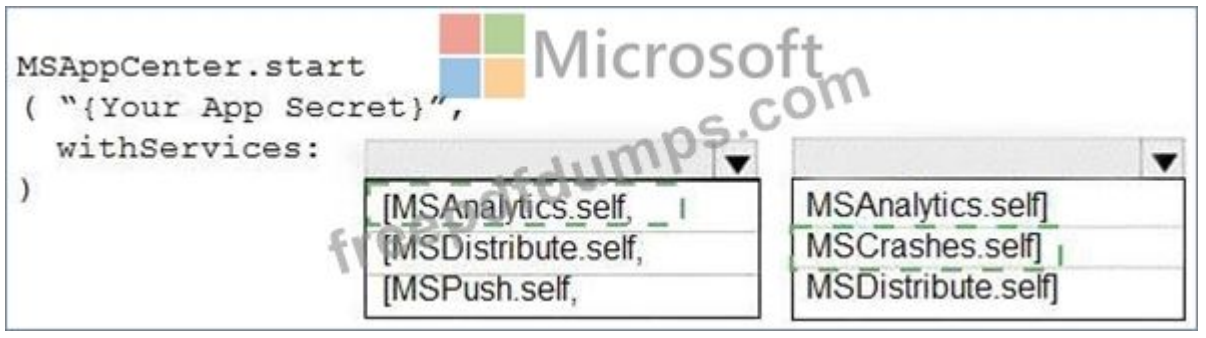
Shared distribution groups are private or public distribution groups that are shared across multiple apps in a single organization.

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

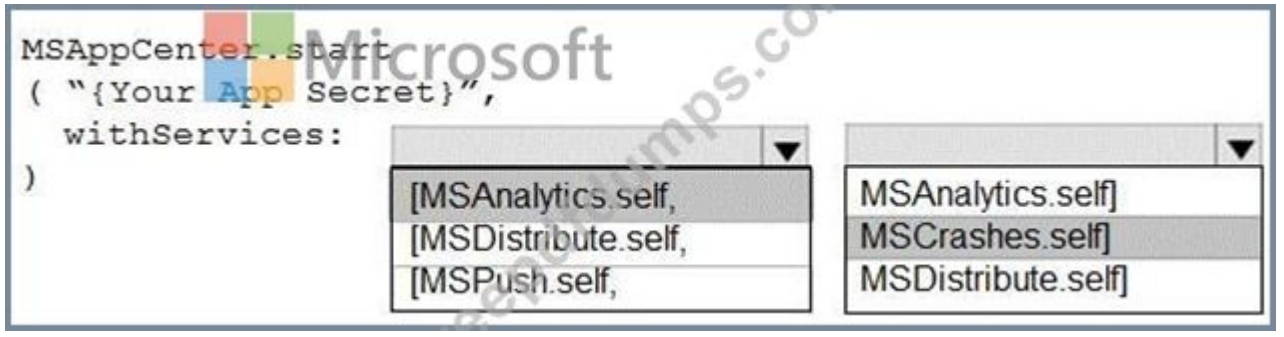
NEW QUESTION: 165
How should you complete the code to initialize App Center in the mobile application? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection a worth one point.



Answer:



Explanation

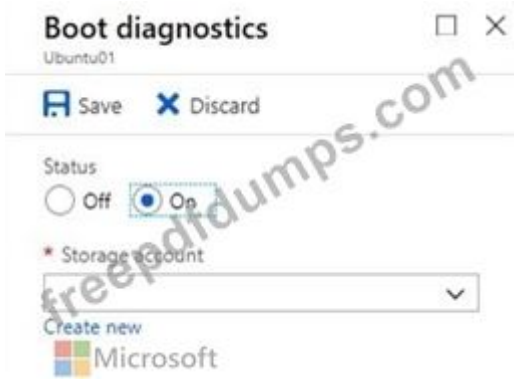


Scenario: Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use.
In order to use App Center, you need to opt in to the service(s) that you want to use, meaning by default no services are started and you will have to explicitly call each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

NEW QUESTION: 166
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a prefect in Azure DevOps for a new web application.
You need to ensure that when code is checked in, a build runs automatically.
Solution: from the Triggers tab of the build pipeline, you select Enable continuous integration Does the meet the goal?
A. No

B. Yes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 167
You need to create and configure an Azure Storage account named az400lod11566895stor in a resource group named RG1lod11566895 to store the boot diagnostics for a virtual machine named VM1.
To complete this task, sign in to the Microsoft Azure portal.
A. Step 1: To create a general-purpose v2 storage account in the Azure portal, follow these steps:
* On the Azure portal menu, select All services. In the list of resources, type Storage Accounts. As you begin typing, the list filters based on your input. Select Storage Accounts.
* On the Storage Accounts window that appears, choose Add.
* Select the subscription in which to create the storage account.
* Under the Resource group field, select RG1lod11588895
* Next, enter a name for your storage account named: az400lod11566895stor
* Select Create.
Step 2: Enable boot diagnostics on existing virtual machine
To enable Boot diagnostics on an existing virtual machine, follow these steps:
1. Sign in to the Azure portal, and then select the virtual machine VM1.
2. In the Support + troubleshooting section, select Boot diagnostics, then select the Settings tab.
3. In Boot diagnostics settings, change the status to On, and from the Storage account drop-down list, select the storage account az400lod11588895stor.
4. Save the change.



You must restart the virtual machine for the change to take effect.
B. Step 1: To create a general-purpose v2 storage account in the Azure portal, follow these steps:
* On the Azure portal menu, select All services. In the list of resources, type Storage Accounts. As you begin typing, the list filters based on your input. Select Storage Accounts.

* On the Storage Accounts window that appears, choose Add.
* Select the subscription in which to create the storage account.
* Under the Resource group field, select RG1lod11566895
* Next, enter a name for your storage account named: az400lod11566895stor
* Select Create.

Step 2: Enable boot diagnostics on existing virtual machine

To enable Boot diagnostics on an existing virtual machine, follow these steps:

1. Sign in to the Azure portal, and then select the virtual machine VM1.
2. In the Support + troubleshooting section, select Boot diagnostics, then select the Settings tab.
3. In Boot diagnostics settings, change the status to On, and from the Storage account drop-down list, select the storage account az400lod11566895stor.
4. Save the change.

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

Answer: B (LEAVE A REPLY)

Reference:

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

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

NEW QUESTION: 168

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 (LEAVE A REPLY)

Topic 1, Overview

Existing Environment

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

Application Architecture

The company' s primary application is a single monolithic retirement fund management system based on ASP.NE T web forms that use logic

written in V8.NET. Some new sections of the application are written in C#.
Variations of the application are created for individual customers. Currently, there are more than 80 have code branches in the application's code base.
The application was developed by using Microsoft Visual Studio. Source code is stored in Team Foundation Server (TFS) in the main office. The branch offices access of the source code by using TFS proxy servers.
Architectural Issues
Litware focuses on writing new code for customers. No resources are provided to refactor or remove existing code. Changes to the code base take a long time, AS dependencies are not obvious to individual developers.
Merge operations of the code often take months and involve many developers. Code merging frequently introduces bugs that are difficult to locate and resolve.
Customers report that ownership costs of the retirement fund management system increase continually. The need to merge unrelated code makes even minor code changes expensive.
Requirements
Planned Changes
Litware plans to develop a new suite of applications for investment planning. The investment planning Applications will require only minor integration with the easting retirement fund management system.
The investment planning applications suite will include one multi-tier web application and two iOS mobile applications. One mobile application will be used by employees; the other will be used by customers.
Litware plans to move to a more agile development methodology. Shared code will be extracted into a series of package.
Litware has started an internal cloud transformation process and plans to use cloud based services whenever suitable.
Litware wants to become proactive m detecting failures, rather than always waning for customer bug reports.
Technical Requirements
The company's investment planning applications suite must meet the following technical requirements:
* New incoming connections through the firewall must be minimized.
* Members of a group named Developers must be able to install packages.
* The principle of least privilege must be used for all permission assignments
* A branching strategy that supports developing new functionality in isolation must be used.
* Members of a group named Team leaders must be able to create new packages and edit the permissions of package feeds
* Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use.
* By default, all App Center must be used to centralize the reporting of mobile application crashes and device types in use.
* Code quality and release quality are critical. During release, deployments must not proceed between stages if any active bugs are logged against the release.
* The mobile applications must be able to call the share pricing service of the existing retirement fund management system. Until the system is upgraded, the service will only support basic authentication over HUPS.
* The required operating system configuration tor the test servers changes weekly. Azure Automation State Configuration must be used to ensure that the operating system on each test servers configured the same way when the servers are created and checked periodically.
Current Technical
The test servers are configured correctly when first deployed, but they experience configuration drift over time. Azure Automation State Configuration fails to correct the configurations.
Azure Automation State Configuration nodes are registered by using the following command.

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

NEW QUESTION: 169

Your company deploys applications m Docket containers.

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

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

What should you configure?

A. a task executed in the continuous deployment pipeline and a scheduled task against a running production container.

B. a task executed in the continuous integration pipeline and a scheduled task that analyzes the production container.

C. a task executed in the continuous integration pipeline and a scheduled task that analyzes the image registry

D. manual tasks performed during the planning phase and the deployment phase

Answer: C (LEAVE A REPLY)

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

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

References:

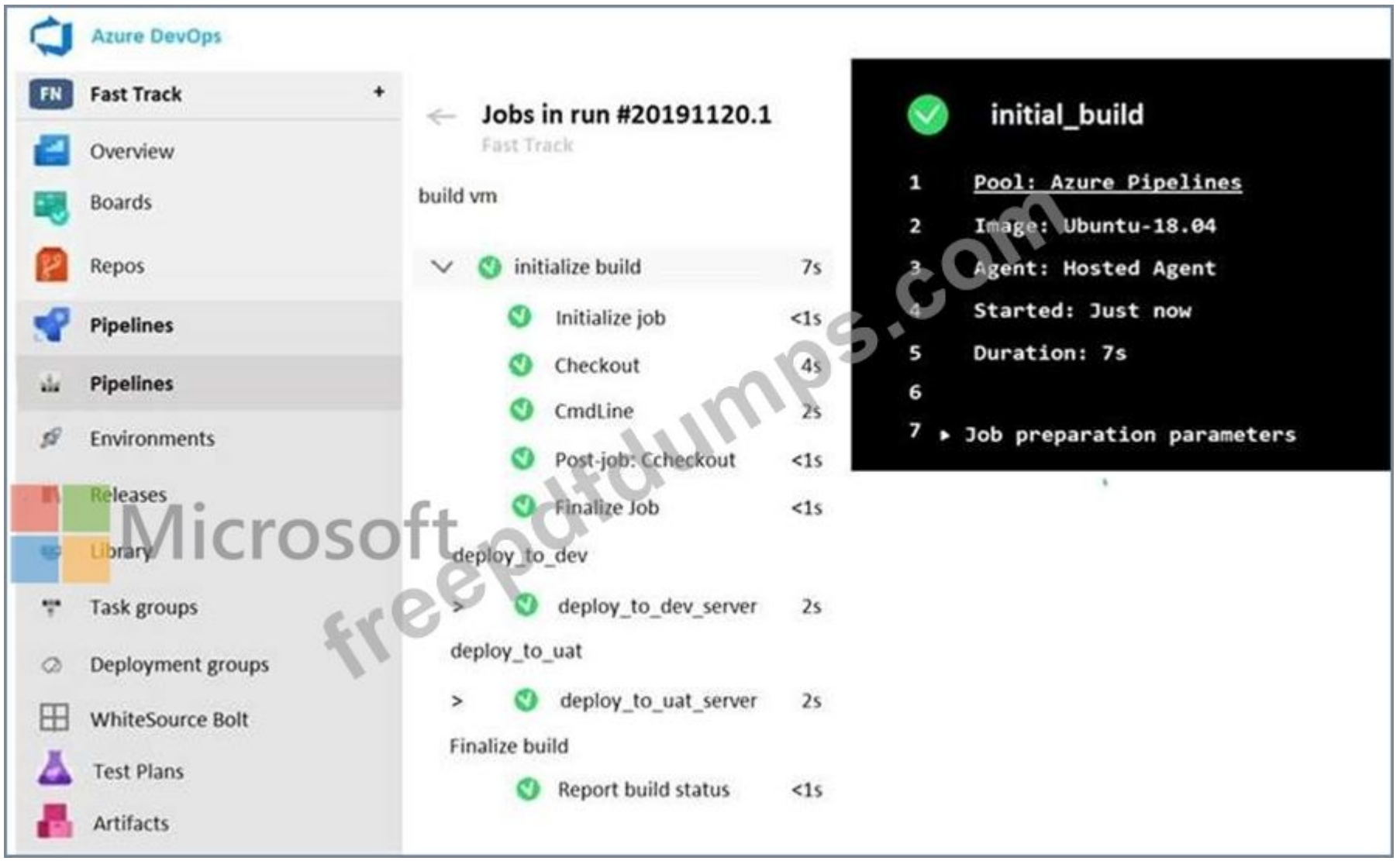
https://docs.microsoft.com/en-us/azure/devops/articles/security-validation-cicd-pipeline?view=vsts

NEW QUESTION: 170

You company uses Azure DevOps to deploy infrastructures to Azure.

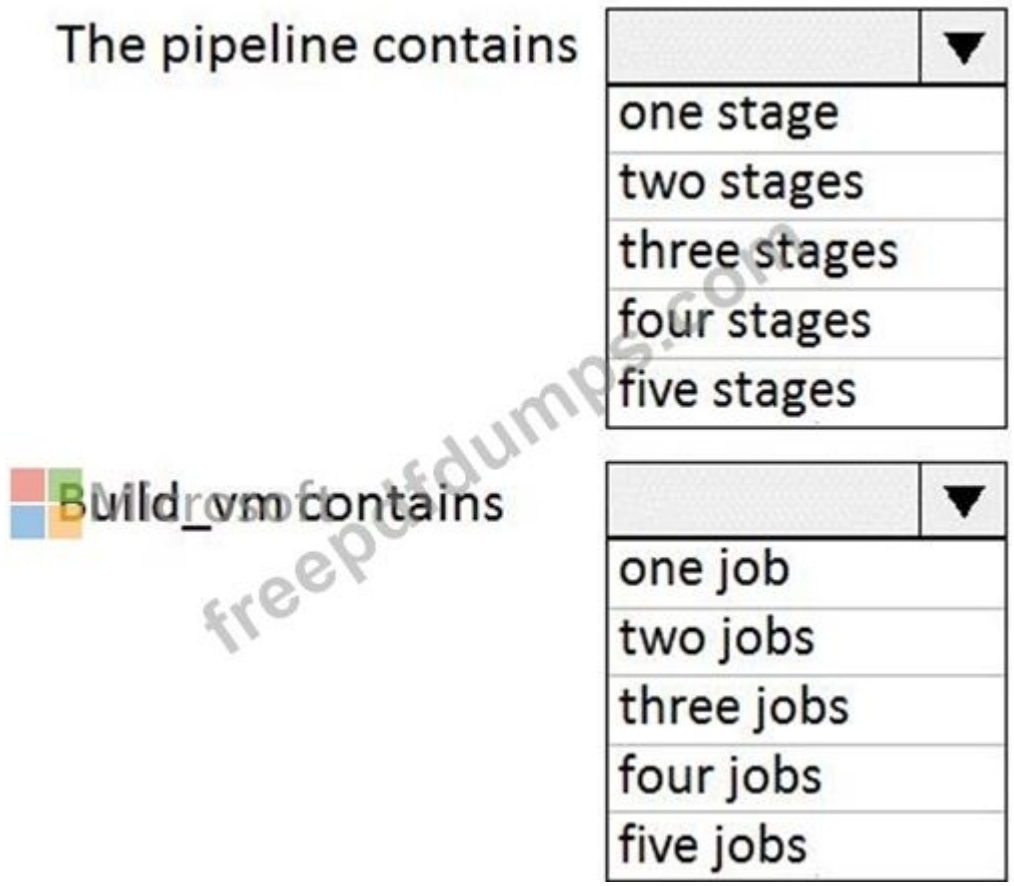
Pipelines are developed by using YAML.

You execute a pipeline and receive the results in the web portal for Azure Pipelines as shown in the following exhibit.

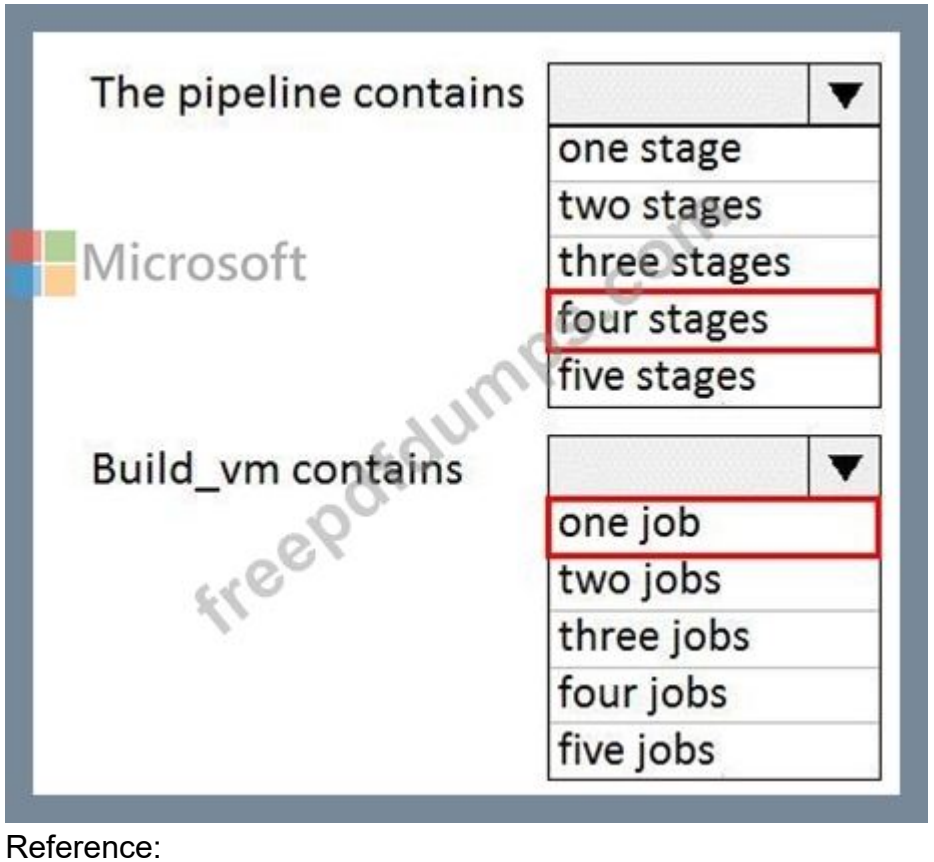


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



Answer:



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

NEW QUESTION: 171

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

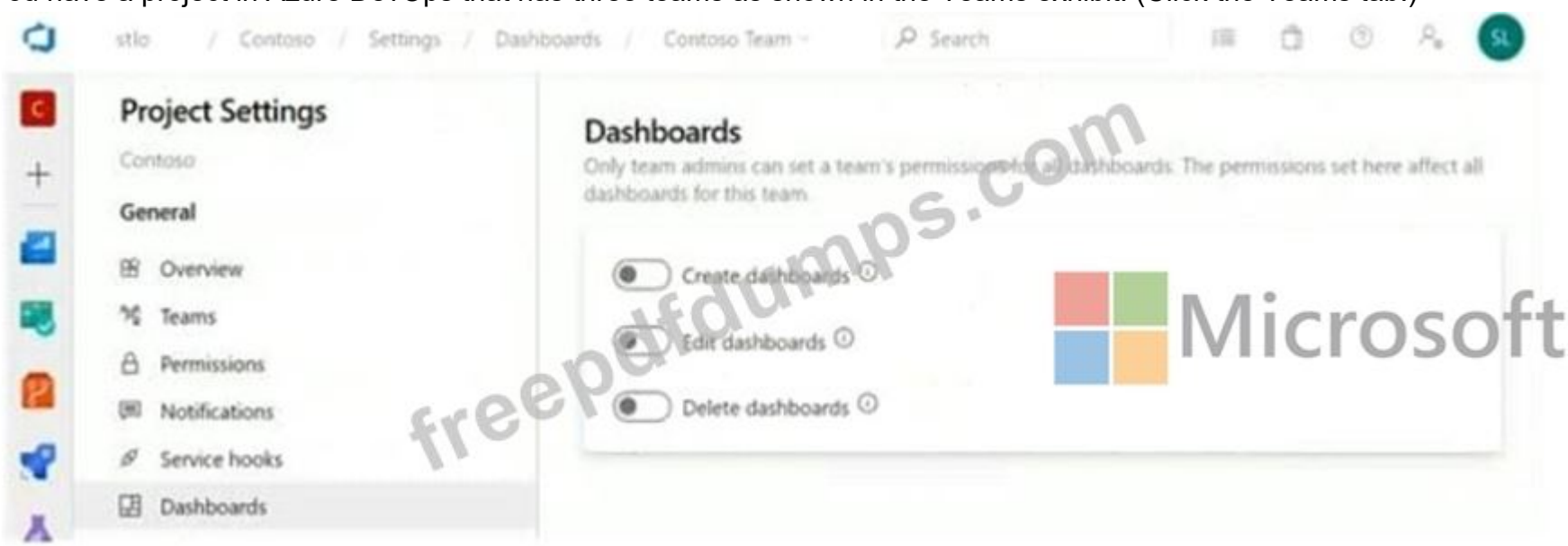
Answer:

Explanation

Every request made against a storage service must be authorized, unless the request is for a blob or container resource that has been made available for public or signed access. One option for authorizing a request is by using Shared Key.
Scenario: The mobile applications must be able to call the share pricing service of the existing retirement fund management system. Until the

system is upgraded, the service will only support basic authentication over HTTPS.
The investment planning applications suite will include one multi-tier web application and two iOS mobile application. One mobile application will be used by employees; the other will be used by customers.
References: https://docs.microsoft.com/en-us/rest/api/storageservices/authorize-with-shared-key

NEW QUESTION: 172
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 Contoso project as shown in the Permissions exhibit (Click the Permissions tab.)

All other permissions have the default values set.

Answer:

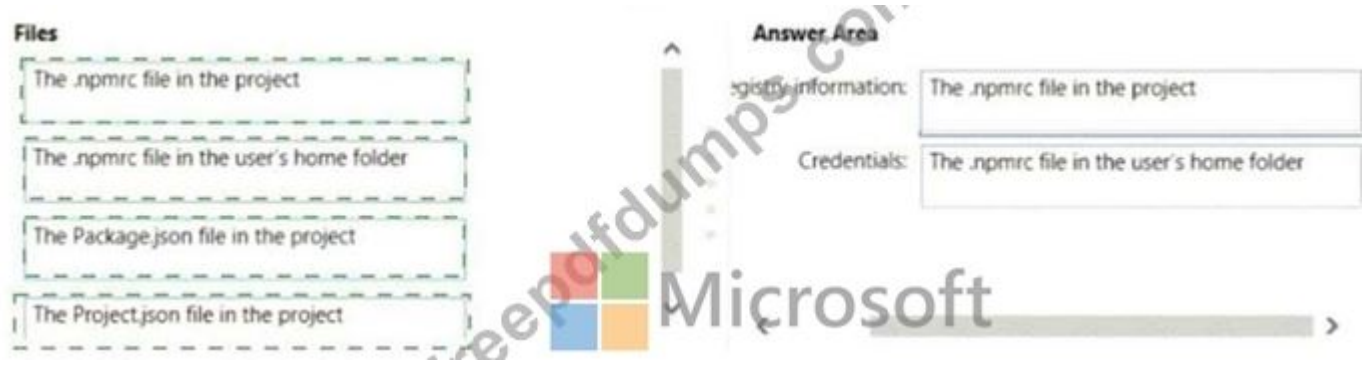
NEW QUESTION: 173

You are implementing a package management solution for a Node.js application by using Azure Artifacts.

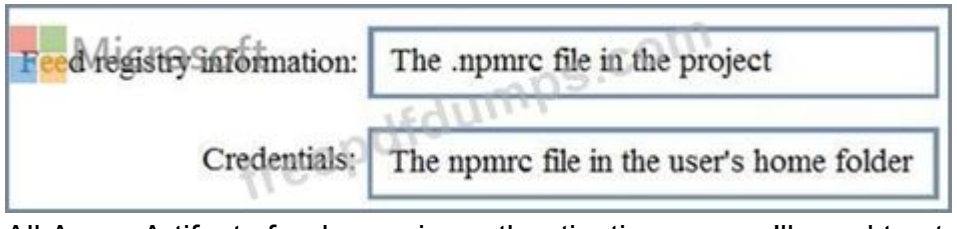
You need to configure the development environment to connect to the package repository. The solution must minimize the likelihood that credentials will be leaked.

Which file should you use to configure each connection? To answer, drag the appropriate files to the correct connections. Each file may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content NOTE: Each correct selection is worth one point.

Answer:



Explanation

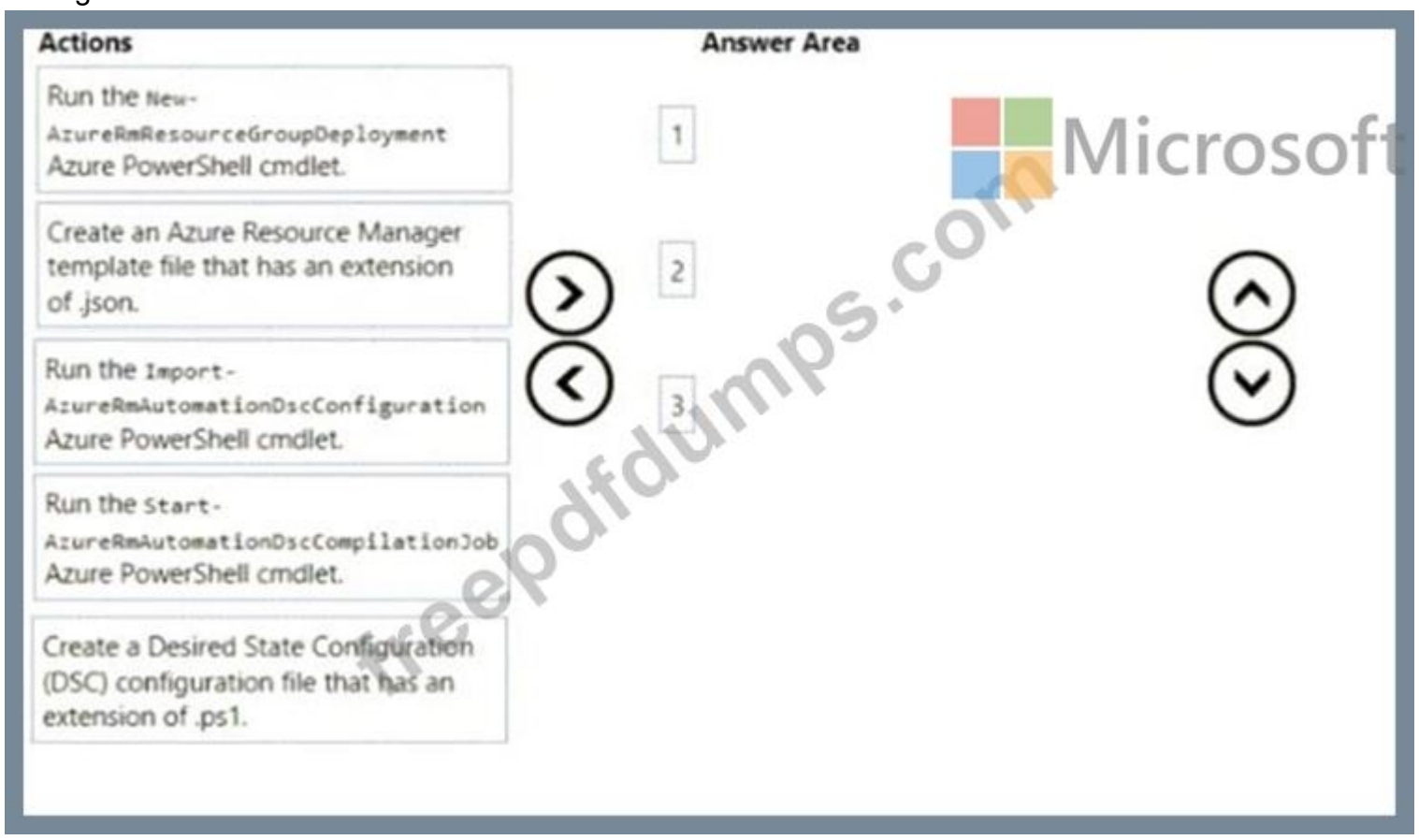


All Azure Artifacts feeds require authentication, so you'll need to store credentials for the feed before you can install or publish packages. npm uses .npmrc configuration files to store feed URLs and credentials. Azure DevOps Services recommends using two .npmrc files.

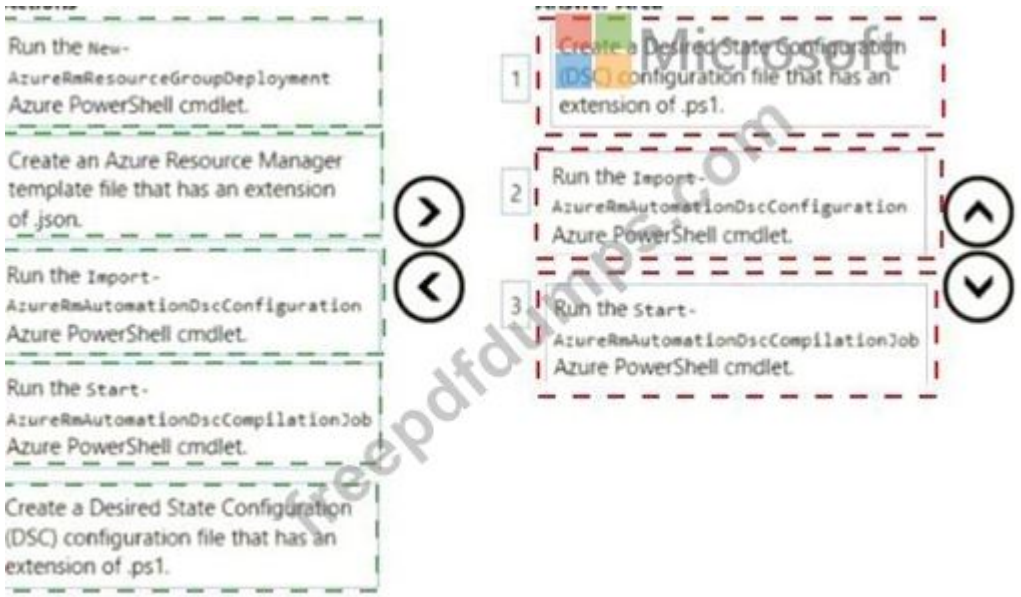
Feed registry information: The .npmrc file in the project

One .npmrc should live at the root of your git repo adjacent to your project's package.json. It should contain a "registry" line for your feed and it should not contain credentials since it will be checked into git.
Credentials: The .npmrc file in the user's home folder
On your development machine, you will also have a .npmrc in $home for Linux or Mac systems or $env.HOME for win systems. This .npmrc should contain credentials for all of the registries that you need to connect to. The NPM client will look at your project's .npmrc, discover the registry, and fetch matching credentials from $home/.npmrc or $env.HOME/.npmrc.
References:
https://docs.microsoft.com/en-us/azure/devops/artifacts/npm/npmrc?view=azure-devops&tabs=windows

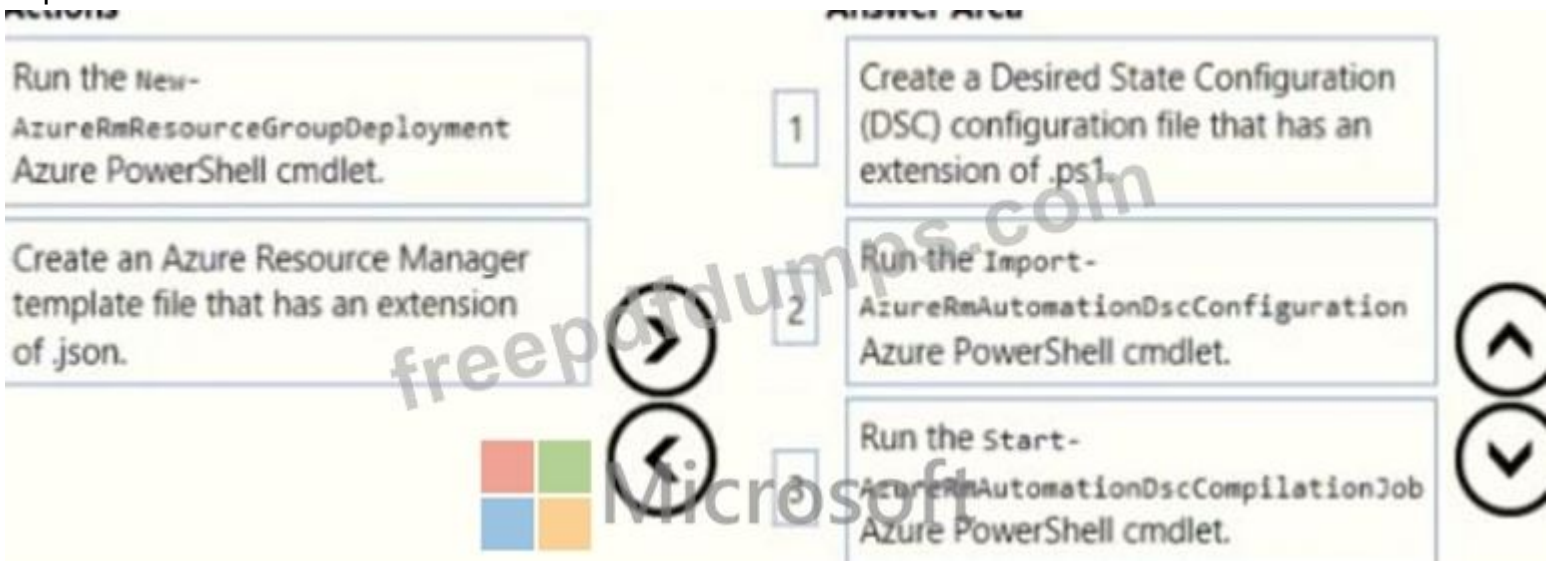
NEW QUESTION: 174
You need to configure Azure Automation for the computers in Pool7.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them m the correct order.



Answer:



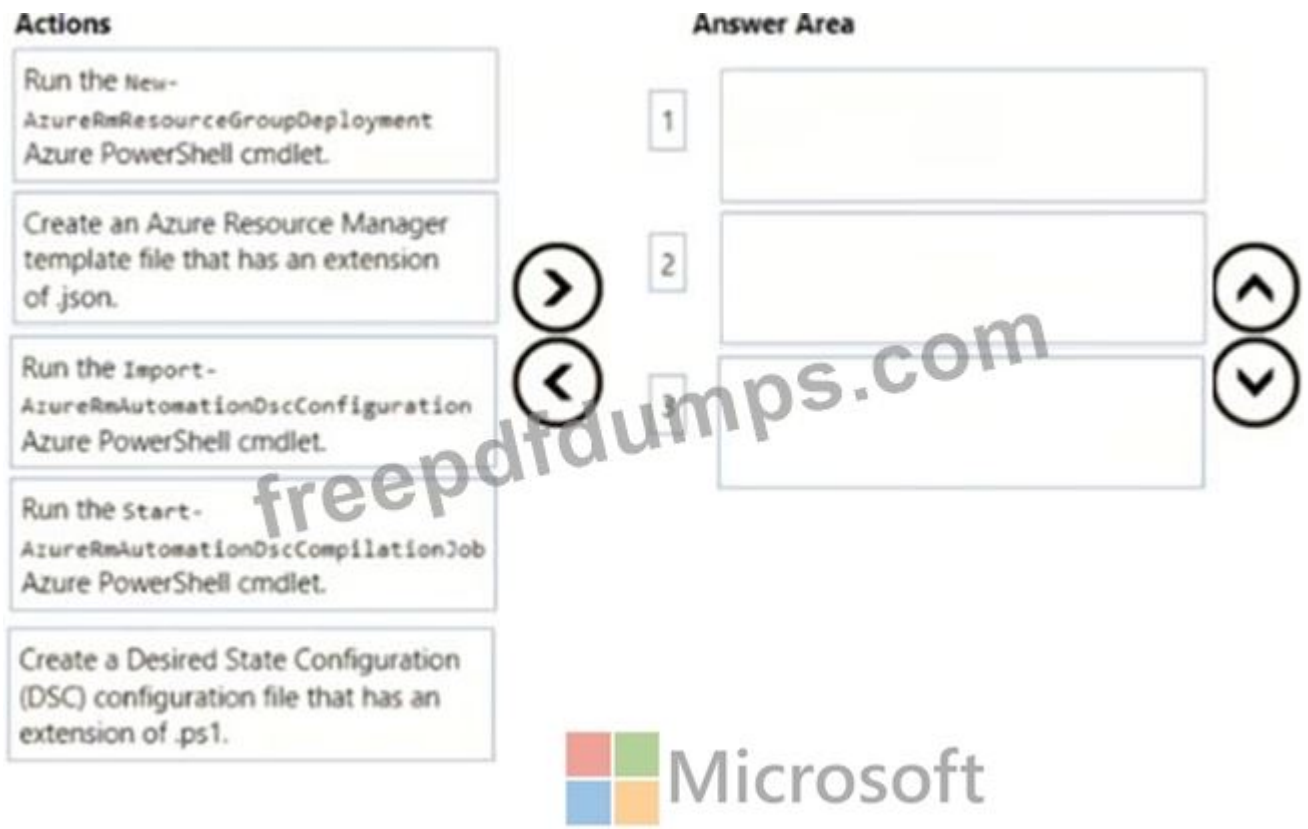
Explanation



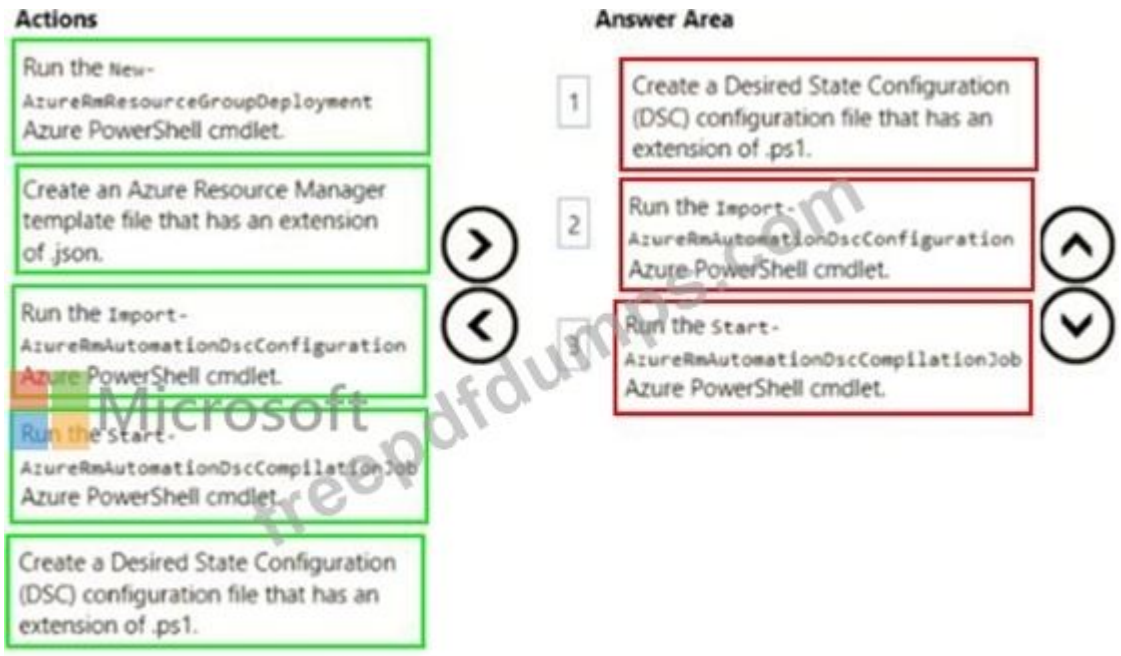
NEW QUESTION: 175

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

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



Answer:



NEW QUESTION: 176

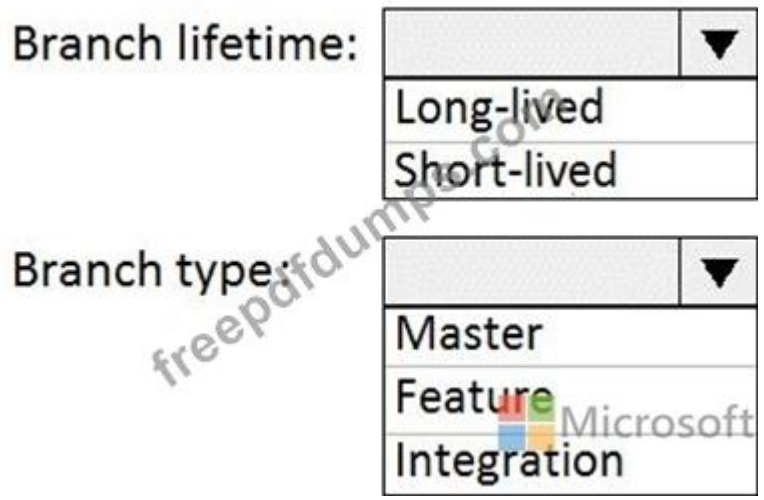
Your company uses Git as a source code control system for a complex app named App1.

You plan to add a new functionality to App1.

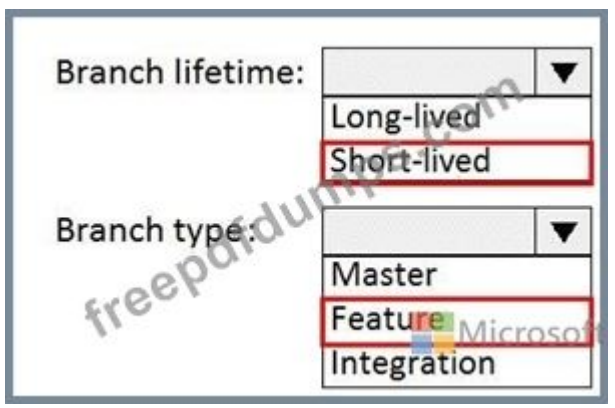
You need to design a branching model for the new functionality.

Which branch lifetime and branch time should you use in the branching model? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Branch lifetime: Short-lived

Branch type: Feature

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

References:

https://gist.github.com/digitaljhelms/4287848

NEW QUESTION: 177

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 Application Insights availability test and alert.

B. Create an Azure Service Health alert for the specific regions.

C. Create an Azure Monitor Availability metric and alert

D. Write an Azure function and deploy the function to the specific regions.

Answer: A (LEAVE A REPLY)

There are three types of Application Insights availability tests:

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

* Multi-step web test
* Custom Track Availability Tests

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

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

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

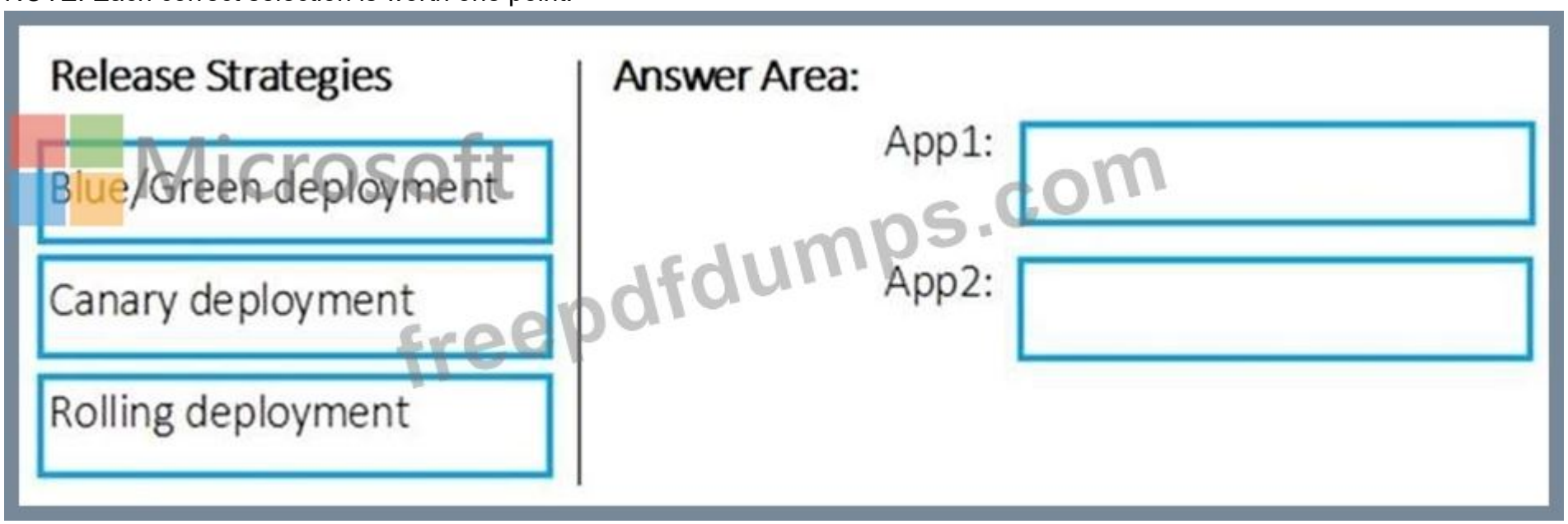
NEW QUESTION: 178

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

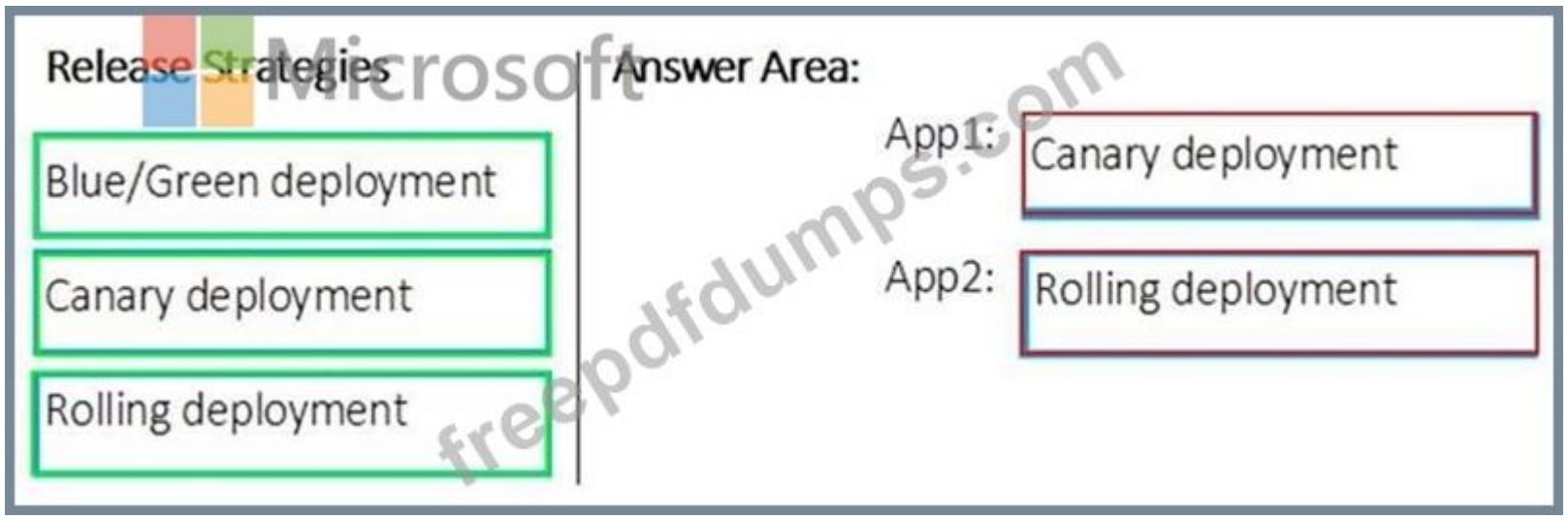
Application name	Goal
App1	Failure of App1 has a major impact on your company. You need a small group of users, who opted in to a testing App1, to test new releases of the application.
App2	You need to minimize the time it takes to deploy new releases of App2, and you must be able to roll back as quickly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

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

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

App1: Canary deployment

With canary deployment, you deploy a new application code in a small part of the production infrastructure. Once the application is signed off for release, only a few users are routed to it. This minimizes any impact.

With no errors reported, the new version can gradually roll out to the rest of the infrastructure.

App2: Rolling deployment:

In a rolling deployment, an application's new version gradually replaces the old one. The actual deployment happens over a period of time. During that time, new and old versions will coexist without affecting functionality or user experience. This process makes it easier to roll back any new component incompatible with the old components.

Incorrect Answers:

Blue/Green deployment

A blue/green deployment is a change management strategy for releasing software code. Blue/green deployments, which may also be referred to as A/B deployments require two identical hardware environments that are configured exactly the same way. While one environment is active and serving end users, the other environment remains idle.

Blue/green deployments are often used for consumer-facing applications and applications with critical uptime requirements. New code is released to the inactive environment, where it is thoroughly tested. Once the code has been vetted, the team makes the idle environment active, typically by adjusting a router configuration to redirect application program traffic. The process reverses when the next software iteration is ready for release.

References:

https://dev.to/mostlyjason/intro-to-deployment-strategies-blue-green-canary-and-more-3a3

NEW QUESTION: 179

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

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

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

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

Does this meet the goal?

A. Yes

B. NO

Answer: A (LEAVE A REPLY)

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

References:

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

NEW QUESTION: 180

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

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

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

You haw a pokey stating that approvals must occur within eight hours.

You discover that deployments only if the approvals take longer than two hours.

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

Solution From Post -deployment conditions, you modify the Timeout setting for post-deployment approvals.

Does this meet the goal?

A. Yes

B. NO

Answer: B (LEAVE A REPLY)

NEW QUESTION: 181

Your company is building a new web application.

You plan to collect feedback from pilot users on the features being delivered.

All the pilot users have a corporate computer that has Google Chrome and the Microsoft Test & Feedback extension installed. The pilot users will test the application by using Chrome.

You need to identify which access levels are required to ensure that developers can request and gather feedback from the pilot users. The solution must use the principle of least privilege.

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

Answer:

Explanation

Box 1: Basic

Assign Basic to users with a TFS CAL, with a Visual Studio Professional subscription, and to users for whom you are paying for Azure Boards & Repos in an organization.

Box 2: Stakeholder

Assign Stakeholders to users with no license or subscriptions who need access to a limited set of features.

Note:

You assign users or groups of users to one of the following access levels:

Basic: provides access to most features

VS Enterprise: provides access to premium features

Stakeholders: provides partial access, can be assigned to unlimited users for free References: https://docs.microsoft.com/en-us/azure/devops/organizations/security/access-levels?view=vsts

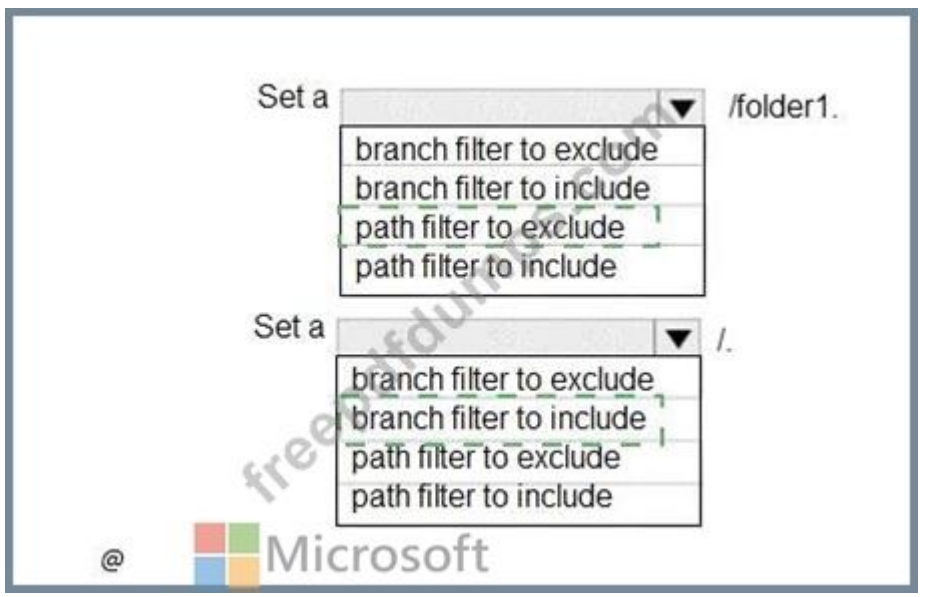
NEW QUESTION: 182

How should you configure the filters for the Project5 trigger? To answer, select the appropriate option in the answer area.

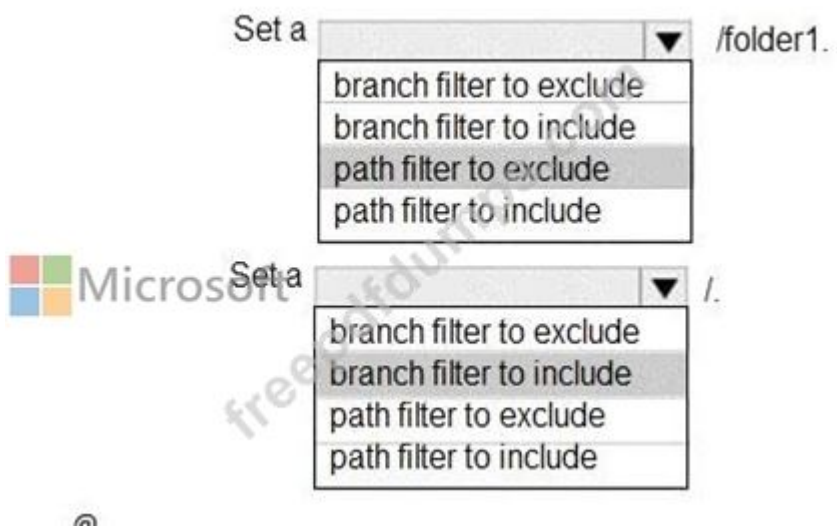
NOTE: Each correct selection is worth one point.

@

Answer:



Explanation



Scenario:

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

NEW QUESTION: 183

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: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
You can authenticate as a GitHub App.
References: https://developer.github.com/apps/building-github-apps/authenticating-with-github-apps/ Question Set 1

NEW QUESTION: 184
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. Create a membership database in an Azure SQL database.
B. Assign an enterprise application to users and groups.
C. Create an app registration in Azure AD.
D. Configure the application to use a SAML endpoint.
E. Create a new OAuth token from the application.
Answer: (SHOW ANSWER)
Explanation
Register your application to use Azure Active Directory. Registering the application means that your developers can use Azure AD to authenticate users and request access to user resources such as email, calendar, and documents.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/developer-guidance-for-integrating-applica
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v2-aspnet-webapp

NEW QUESTION: 185
Your company has a project in Azure DevOps.
You plan to create a release pipeline that will deploy resources by using Azure Resource Manager templates. The templates will reference secrets stored in Azure Key Vault.
You need to recommend a solution for accessing the secrets stored in the key vault during deployments. The solution must use the principle of least privilege.
What should you include in the recommendation? To answer, drag the appropriate configurations to the correct targets. Each configuration may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Box 1: RBAC

Management plane access control uses RBAC.

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

* Creating or deleting a key vault.
* Getting a list of vaults in a subscription.
* Retrieving Key Vault properties (such as SKU and tags).
* Setting Key Vault access policies that control user and application access to keys and secrets.

Box 2: RBAC

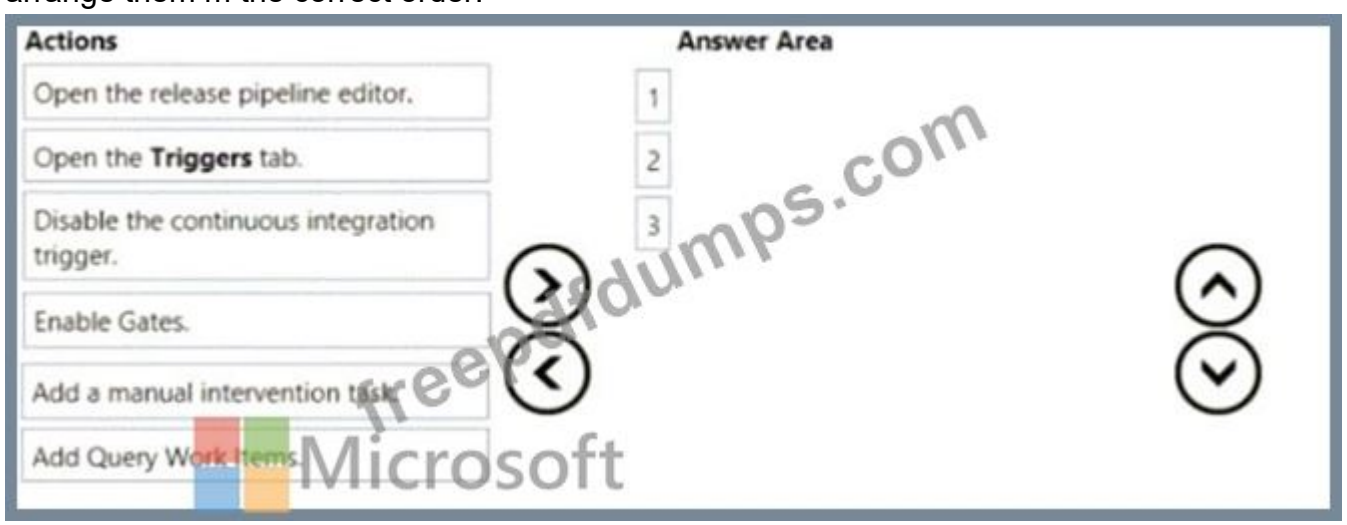
References:

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

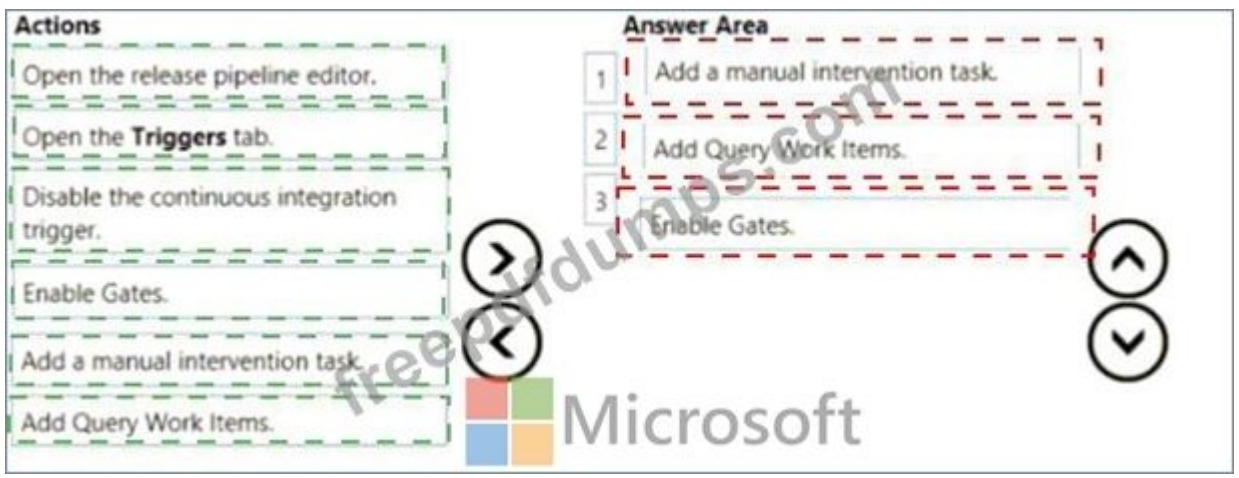
NEW QUESTION: 186

You need to implement Project6.

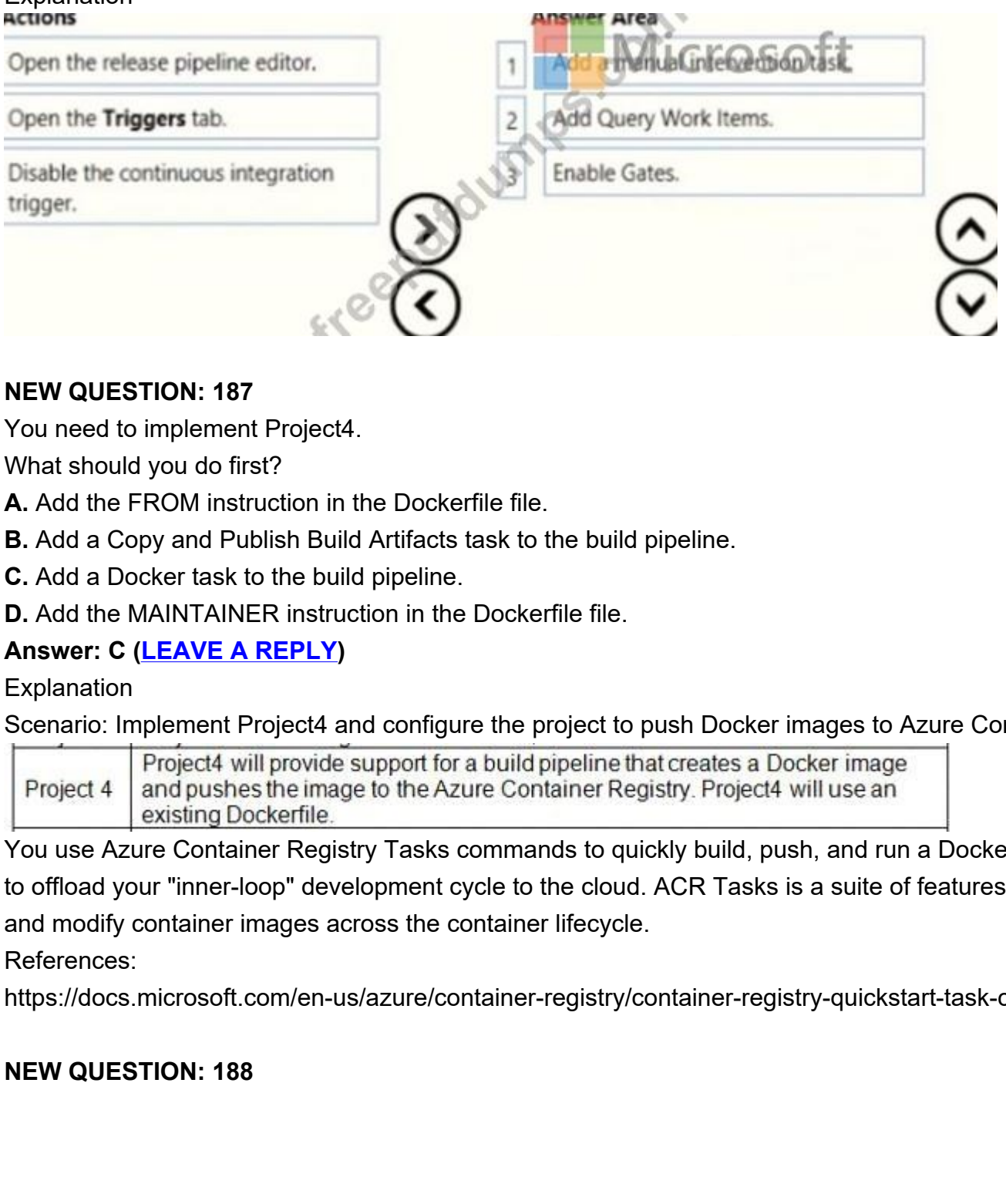
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them m the correct order.



Answer:



Explanation



NEW QUESTION: 187

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 (LEAVE A REPLY)

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.

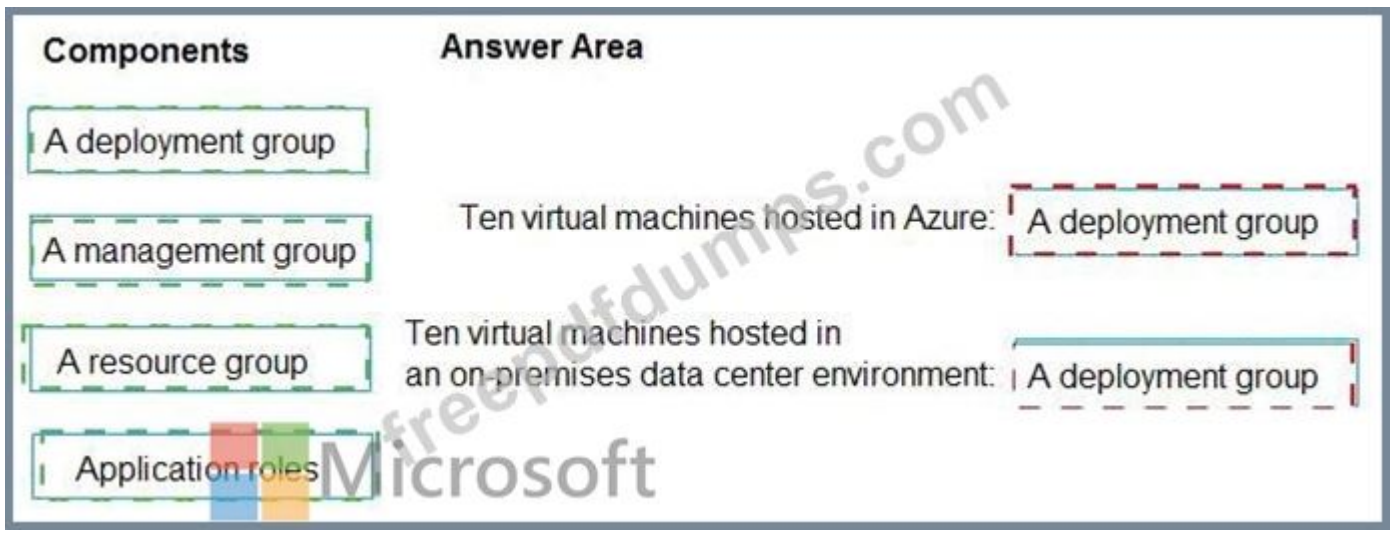
References:

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-quickstart-task-cli

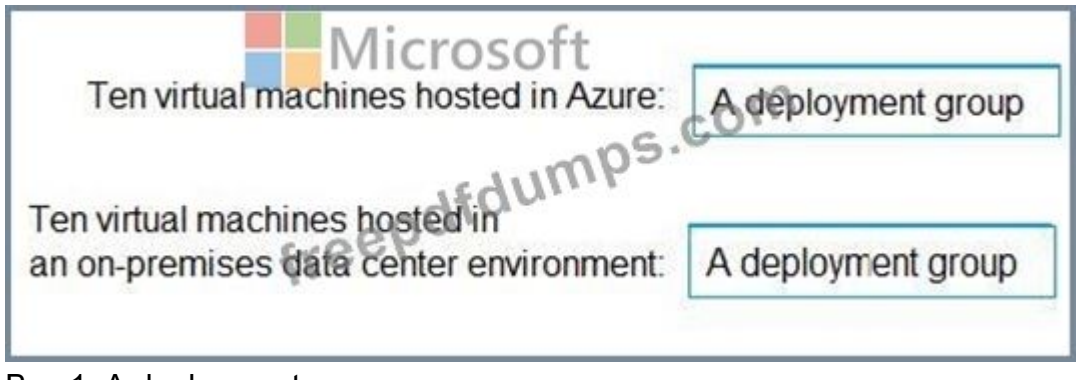
NEW QUESTION: 188

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

Answer:



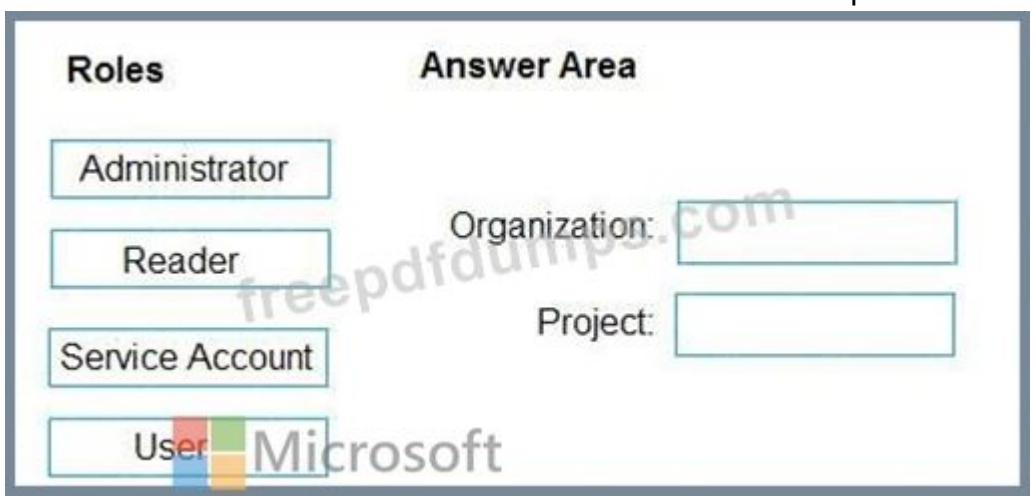
Explanation



Box 1: A deployment group
When authoring an Azure Pipelines or TFS Release pipeline, you can specify the deployment targets for a job using a deployment group.
If the target machines are Azure VMs, you can quickly and easily prepare them by installing the Azure Pipelines Agent Azure VM extension on each of the VMs, or by using the Azure Resource Group Deployment task in your release pipeline to create a deployment group dynamically.

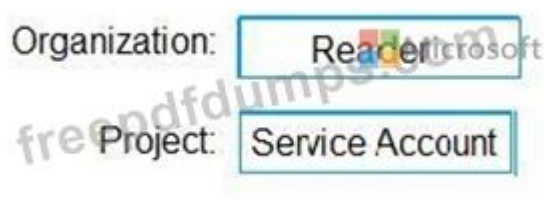
Box 2: A deployment group
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deployment-groups

NEW QUESTION: 189
You need to configure access to Azure DevOps Agent pools to meet the forwarding requirements:
* Use a project agent pool when authoring build release pipelines.
* View the agent pool and agents of the organization.
* Use the principle of least privilege.
Which role memberships are required for the Azure 0e%Oos organization and the project? To answer, drag the appropriate role membership to the correct targets. Each role membership may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to content NOTE: Each correct selection is worth one point.



Answer:

Explanation

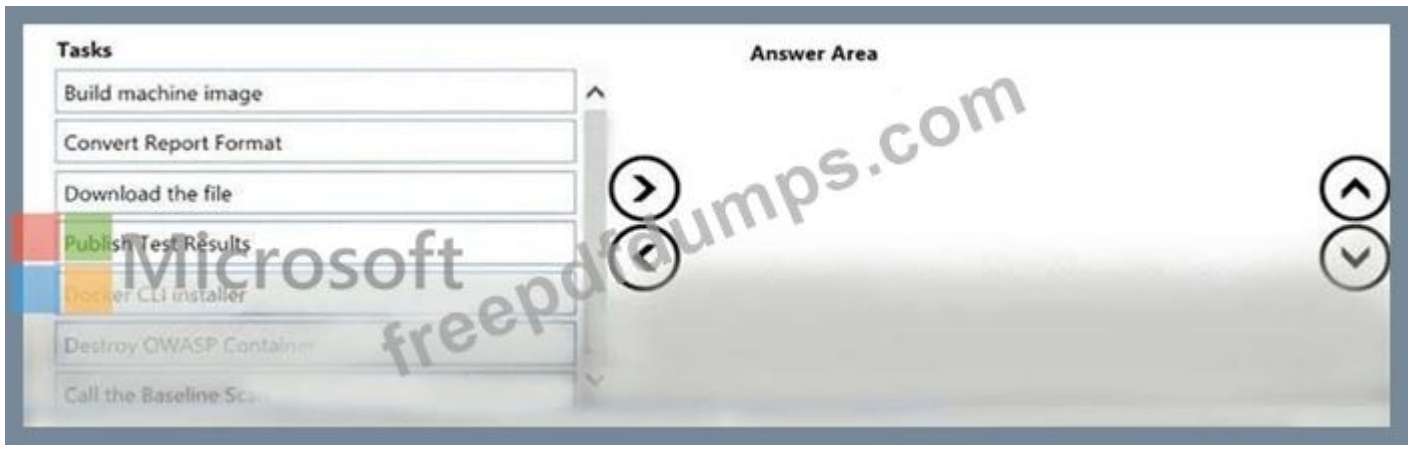


Box 1: Reader
Members of the Reader role can view the organization agent pool as well as agents. You typically use this to add operators that are responsible for monitoring the agents and their health.

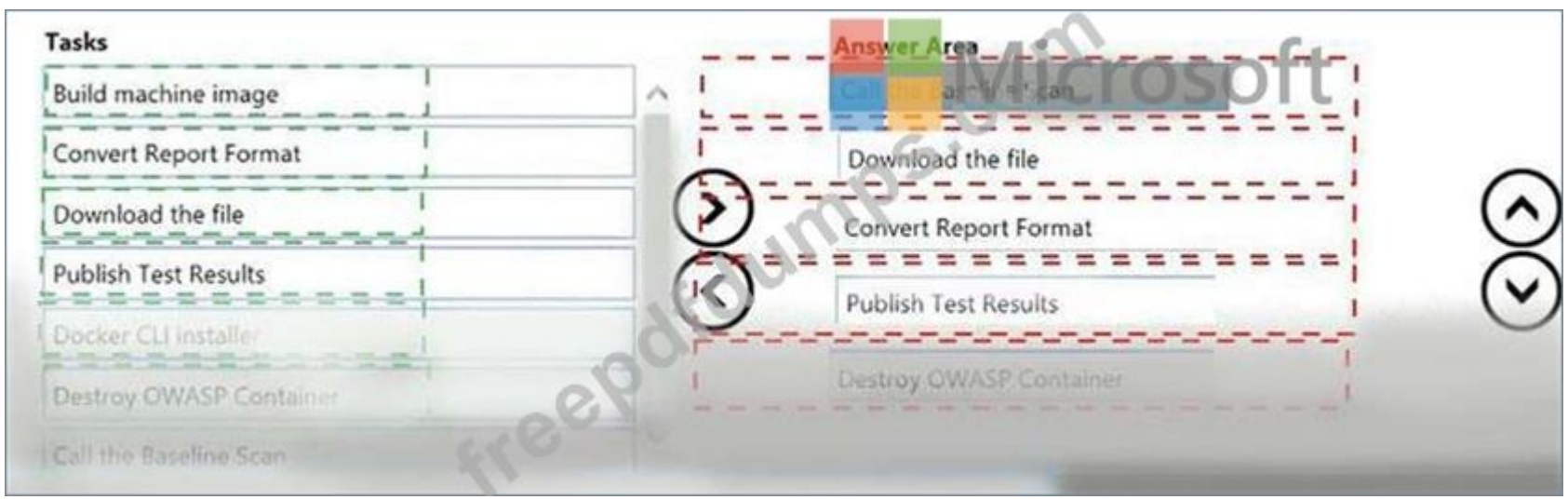
Box 2: Service account
Members of the Service account role can use the organization agent pool to create a project agent pool in a project. If you follow the guidelines above for creating new project agent pools, you typically do not have to add any members here.

NEW QUESTION: 190
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.



Answer:



Explanation

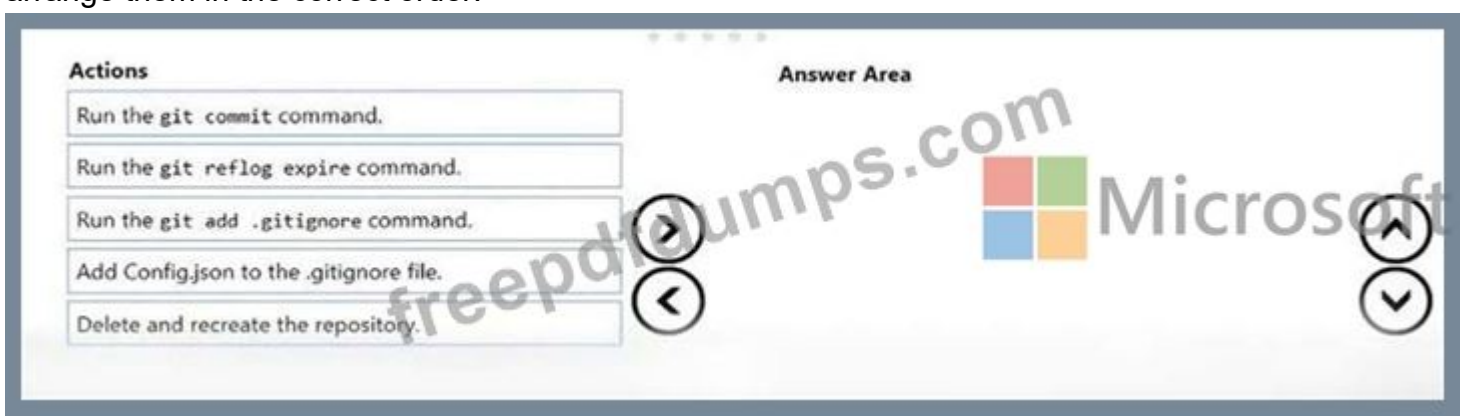
NEW QUESTION: 191

You manage the Git repository for a large enterprise application.

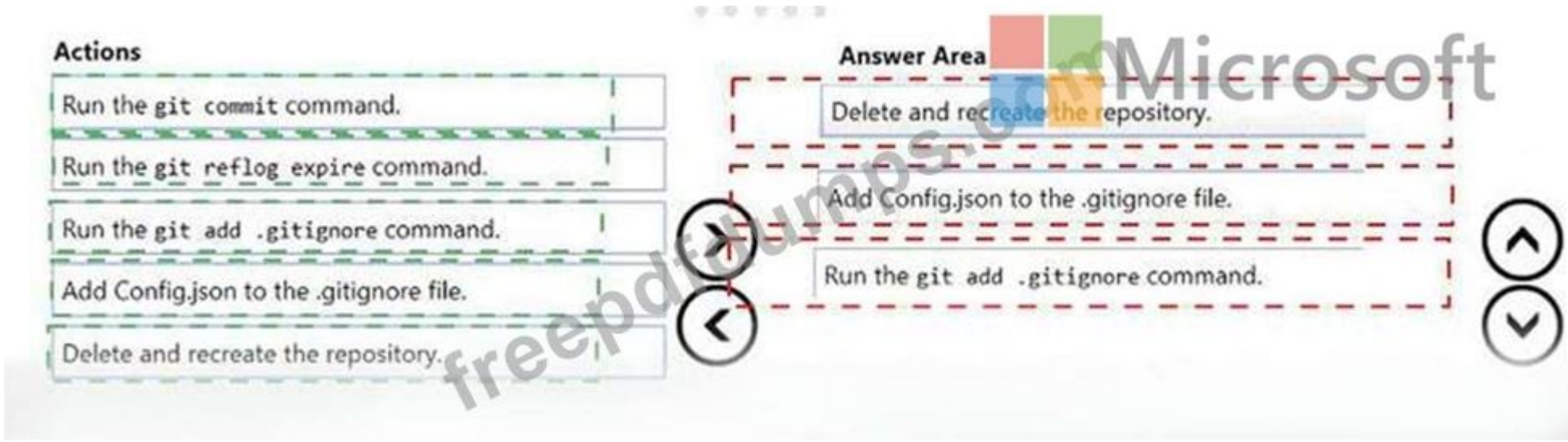
During the development of the application, you use a file named Config.json.

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.



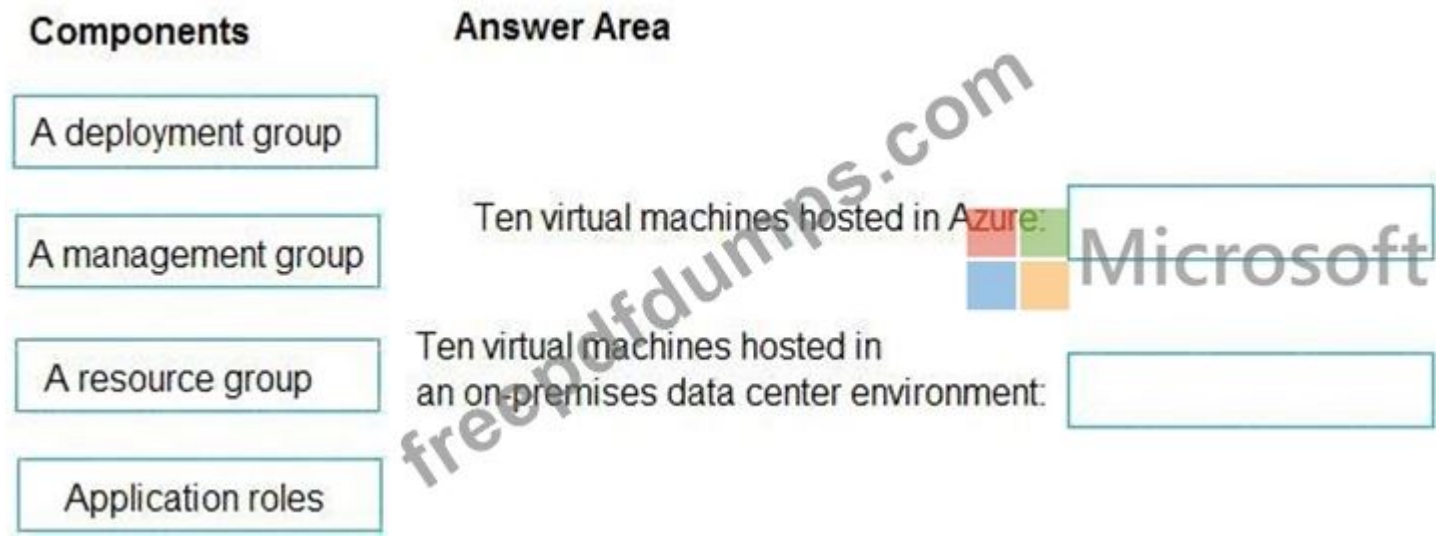
Answer:



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/

NEW QUESTION: 192
Your company plans to deploy an application to the following endpoints:
* Ten virtual machines hosted in Azure
* Ten virtual machines hosted in an on-premises data center environment All the virtual machines have the Azure Pipelines agent.
You need to implement a release strategy for deploying the application to the endpoints.
What should you recommend using to deploy the application to the endpoints? To answer, drag the appropriate components to the correct endpoints. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:

Explanation

Box 1: A deployment group

When authoring an Azure Pipelines or TFS Release pipeline, you can specify the deployment targets for a job using a deployment group.

If the target machines are Azure VMs, you can quickly and easily prepare them by installing the Azure Pipelines Agent Azure VM extension on each of the VMs, or by using the Azure Resource Group Deployment task in your release pipeline to create a deployment group dynamically.

Box 2: A deployment group

References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deployment-groups

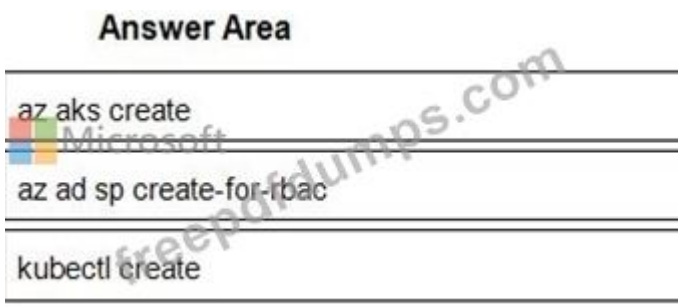
NEW QUESTION: 193

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

You need to recommend a solution for provisioning and connecting to AKS. The solution must ensure that AKS is RBAC-enaWed and uses a custom service principal.

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

Answer:



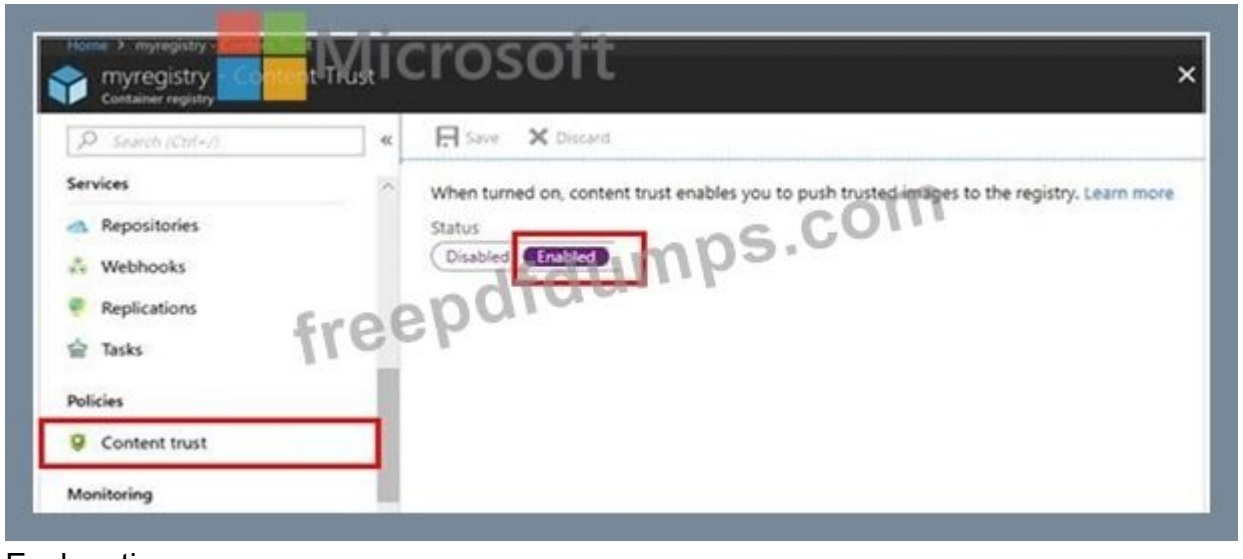
1 - az aks create
2 - az ad sp create-for-rbac
3 - kubectl create
Explanation:
Step 1 : az acr create
An Azure Container Registry (ACR) can also be created using the new Azure CLI.
az acr create
--name <REGISTRY_NAME>
--resource-group <RESOURCE_GROUP_NAME>
--sku Basic
Step 2: az ad sp create-for-rbac
Once the ACR has been provisioned, you can either enable administrative access (which is okay for testing) or you create a Service Principal (sp) which will provide a client_id and a client_secret.
az ad sp create-for-rbac
--
scopes /subscriptions/<SUBSCRIPTION_ID>/resourcegroups/<RG_NAME>/providers/Microsoft.ContainerRegistry/registries/<REGISTRY_NAME>
--role Contributor
--name <SERVICE_PRINCIPAL_NAME>
Step 3: kubectl create
Create a new Kubernetes Secret.
kubectl create secret docker-registry <SECRET_NAME>
--docker-server <REGISTRY_NAME>.azurecr.io
--docker-email <YOUR_MAIL>
--docker-username=<SERVICE_PRINCIPAL_ID>
--docker-password <YOUR_PASSWORD>
References:
https://thorsten-hans.com/how-to-use-private-azure-container-registry-with-kubernetes

NEW QUESTION: 194
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 (LEAVE A REPLY)
Explanation/Reference:
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.
Incorrect Answers:
C: We should not wait until deployment. We want to detect the exploits as early as possible.
D: We should wait until the image is in the product container. We want to detect the exploits as early as possible.
References: https://docs.microsoft.com/en-us/azure/devops/articles/security-validation-cicd-pipeline?
view=vsts

NEW QUESTION: 195
You plane to store signed images in an Azure Container Registry instance named az4009940427acr1.
You need to modify the SKU for az4009940427acr1 to support the planned images. The solution must minimize costs.
To complete this task, sign in to the Microsoft Azure portal.
1. Open Microsoft Azure Portal, and select the Azure Container Registry instance named az4009940427acr1.
2. Under Policies, select Content Trust > Enabled > Save.

Answer:



Explanation:

References:

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

NEW QUESTION: 196

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 (LEAVE A REPLY)

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:

C: xcpretty is a fast and flexible formatter for xcodebuild.

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

NEW QUESTION: 197

You have a project in Azure DevOps that uses packages from multiple public feeds. Some of the feeds are unreliable.

You need to consolidate the packages into a single feed.

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

Answer:

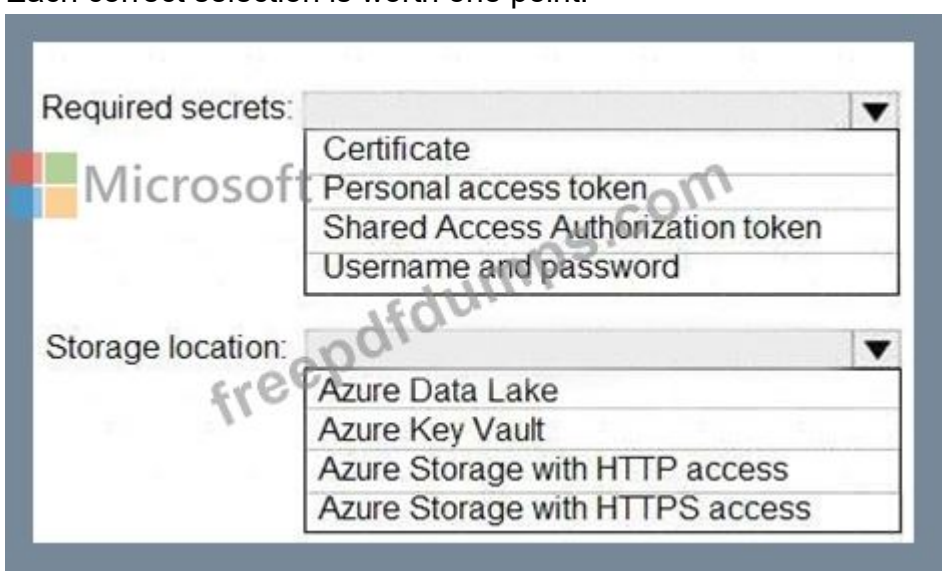
Explanation

NEW QUESTION: 198

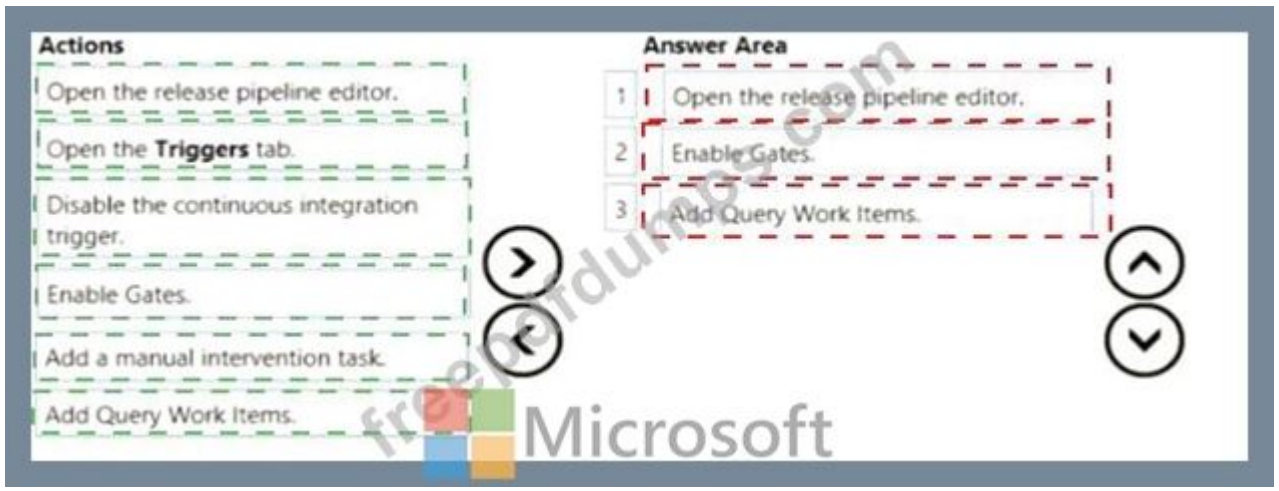
You need to configure a cloud service to store the secrets required by the mobile applications to call the share.

What should you include in the solution? To answer, select the appropriate options m the answer ater, NOTE:

Each correct selection is worth one point.



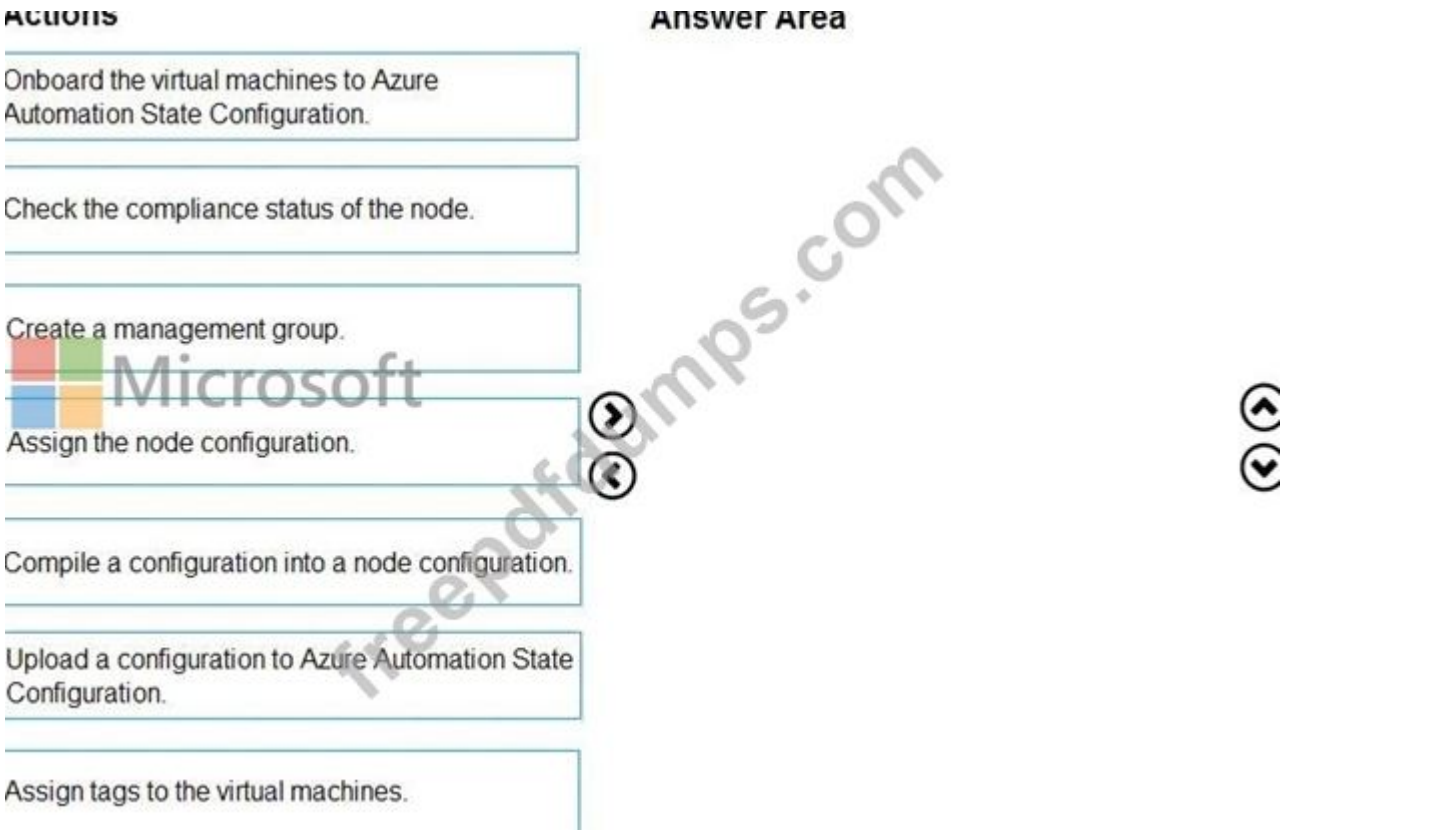
Answer:



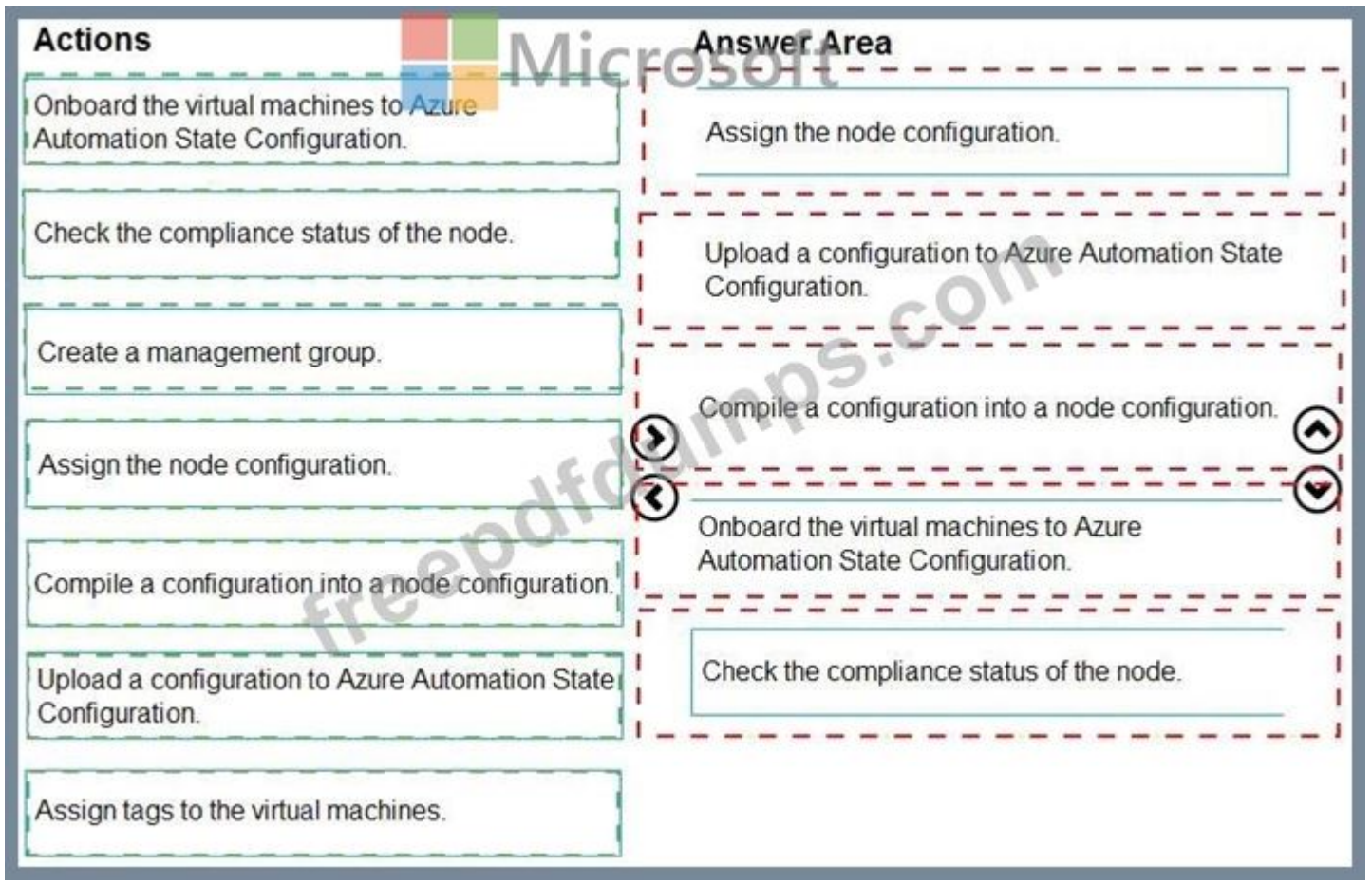
Explanation

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

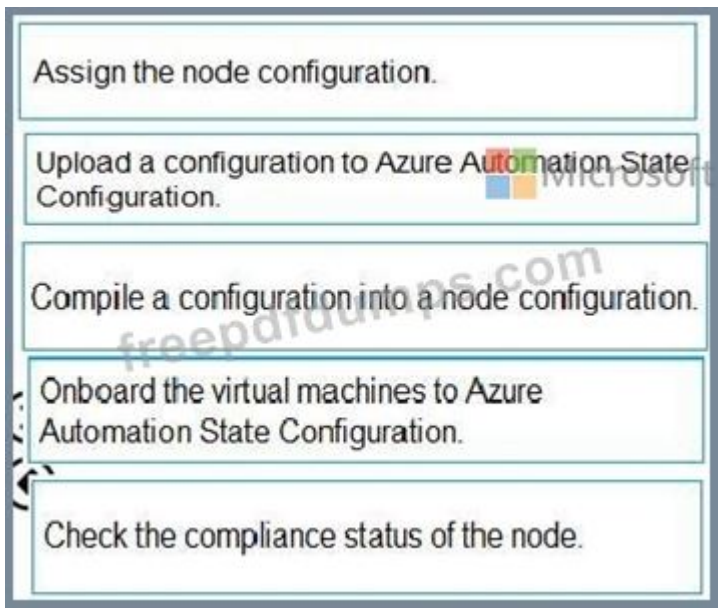
NEW QUESTION: 199
You need to use Azure Automation Sure Configuration to manage the ongoing consistency of virtual machine configurations.
Which five actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
NOTE: More than one order of answer choices in correct. You writ receive credit for any of the orders you select.



Answer:



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

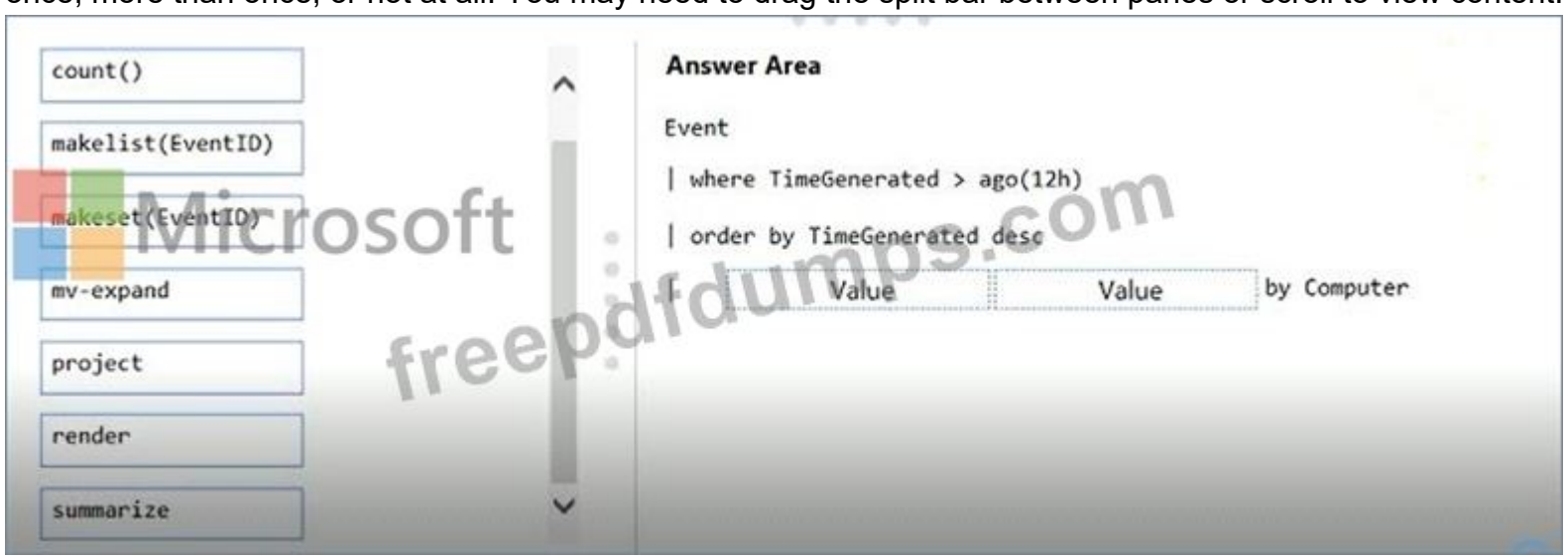
NEW QUESTION: 200
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a project in Azure DevOps.
You need to prevent the configuration of the project from changing over time.
Solution: Implement Continuous Assurance for the project.
Does this meet the goal?
A. Yes
B. No

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

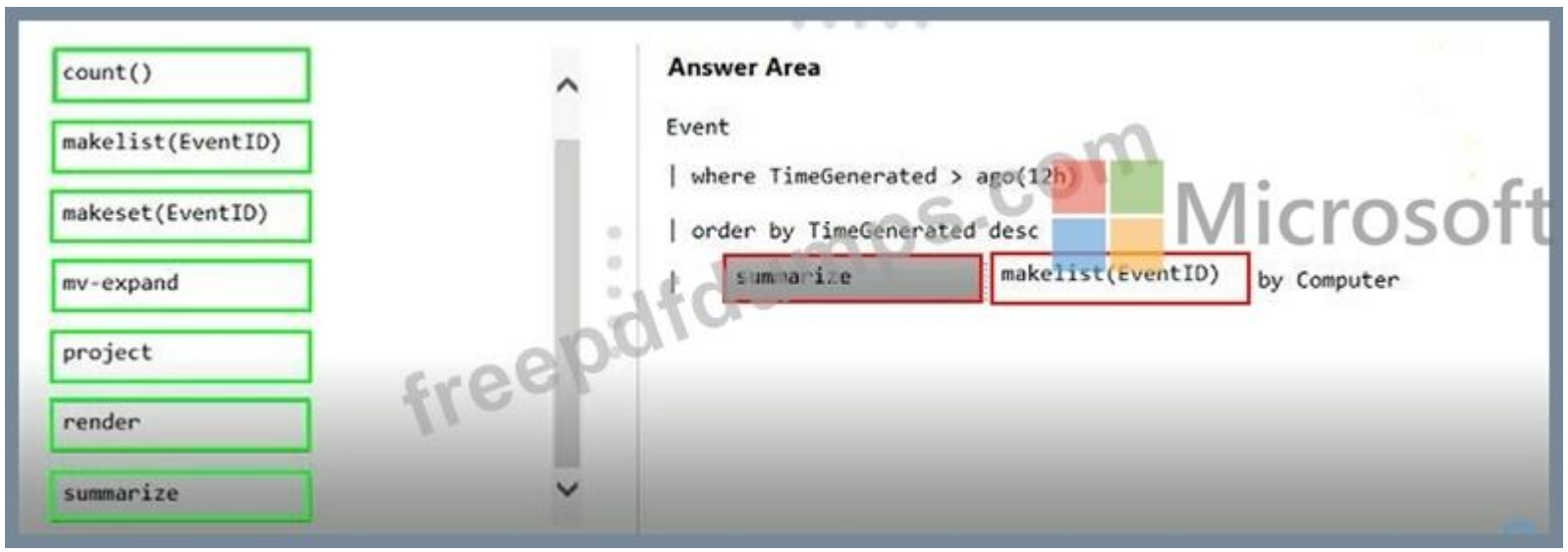
NEW QUESTION: 201
You have several Azure virtual machines that run Windows Server 2019.
You need to identify the distinct event IDs of each virtual machine as shown in the following table.

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.



Answer:



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

NEW QUESTION: 202

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. OpenID

B. GitHub App

C. a personal access token (PAT)

D. SAML

Answer: B (LEAVE A REPLY)

You can authenticate as a GitHub App.

Reference:

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

NEW QUESTION: 203

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.

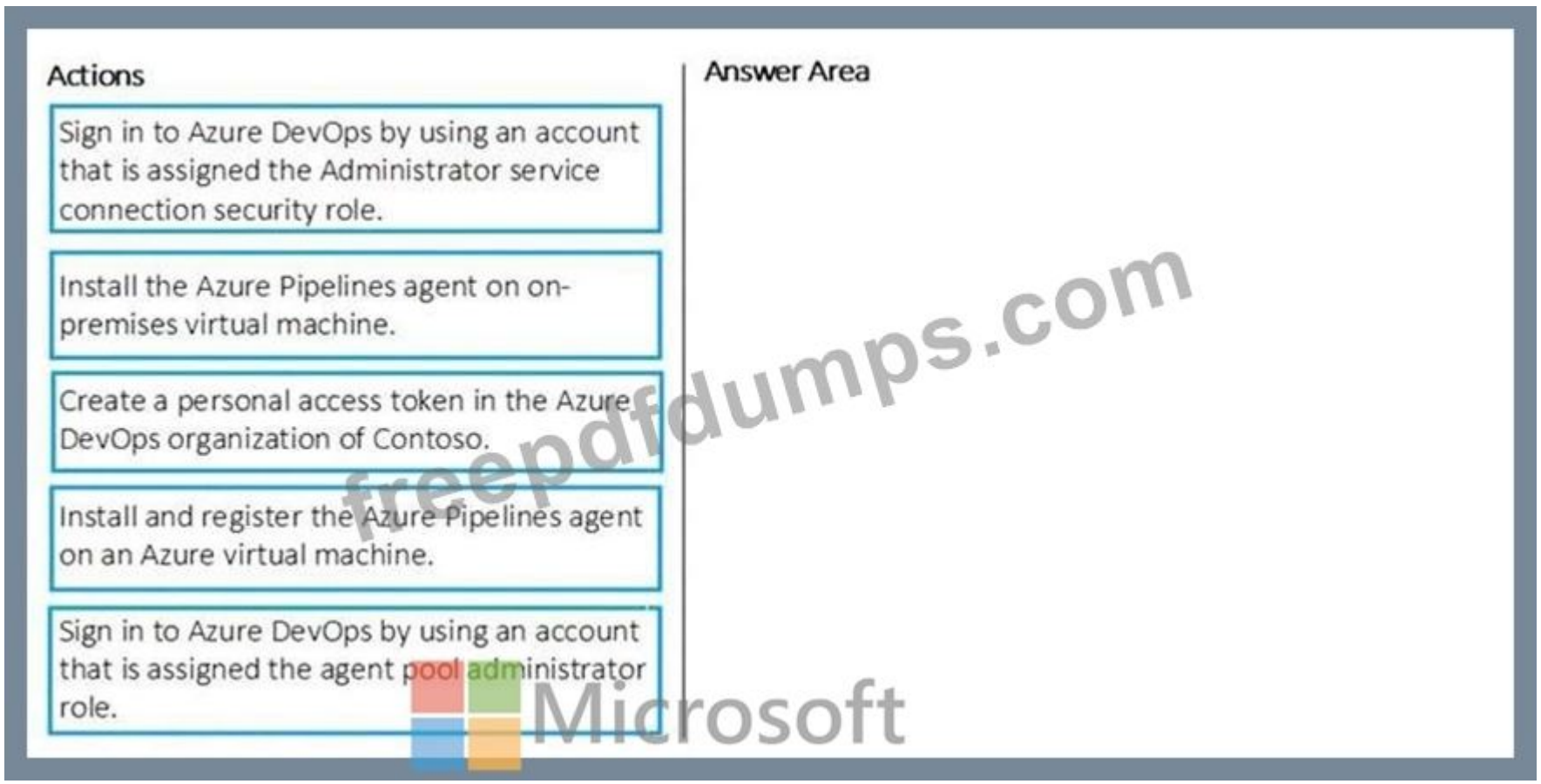
What should you do?

A. Request the Apple ID associated with the user of each device.

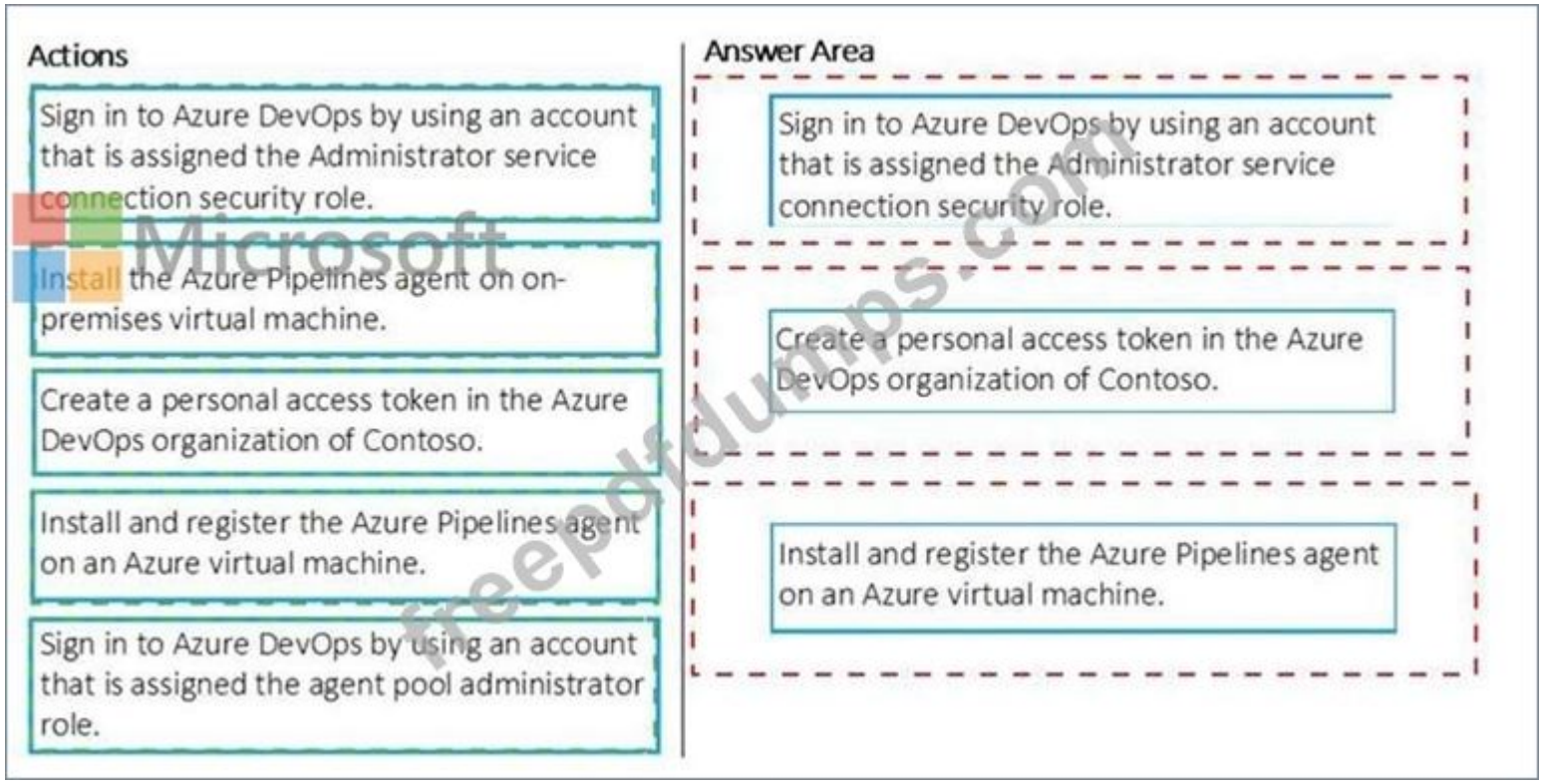
B. Register the devices on the Apple Developer portal.
C. Create an active subscription in App Center Test.
D. Add the device owner to the organization in App Center.
Answer: B (LEAVE A REPLY)
Explanation
When releasing an iOS app signed with an ad-hoc or development provisioning profile, you must obtain 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

NEW QUESTION: 204
Your company has a hybrid cloud between Azure and Azure Stack.
The company uses Azure DevOps for its CI/CD pipelines. Some applications are built by using Erlang and Hack.
You need to ensure that Erlang and Hack are supported as part of the build strategy across the hybrid cloud. The solution must minimize management overhead.
What should you use to execute the build pipeline?
A. AzureDevOps self-hosted agents on Azure DevTest Labs virtual machines.
B. AzureDevOps self-hosted agents on virtual machine that run on Azure Stack
C. AzureDevOps self-hosted agents on Hyper-V virtual machines
D. a Microsoft-hosted agent
Answer: B (LEAVE A REPLY)
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

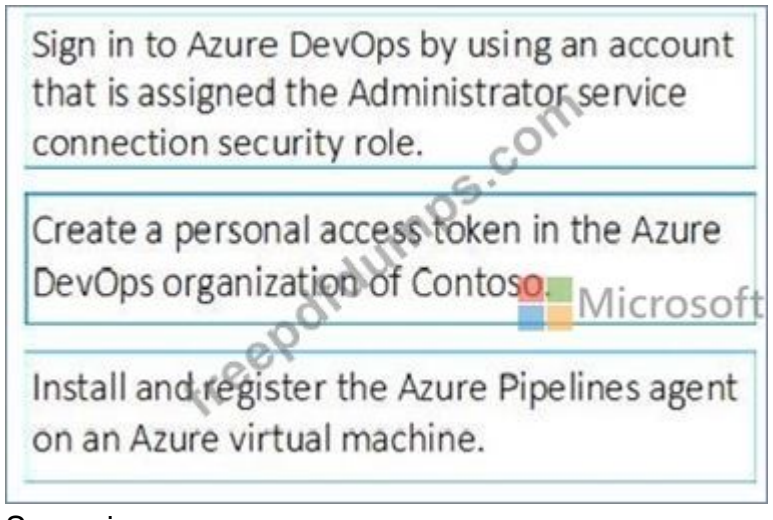
NEW QUESTION: 205
You need to recommend a procedure to implement the build agent for Project1.
Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation



Scenario:

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

Step 1: Sign in to Azure Devops by using an account that is assigned the Administrator service connection security role.

Note: Under Agent Phase, click Deploy Service Fabric Application. Click Docker Settings and then click Configure Docker settings. In Registry Credentials Source, select Azure Resource Manager Service Connection. Then select your Azure subscription.

Step 2: Create a personal access token..

A personal access token or PAT is required so that a machine can join the pool created with the Agent Pools (read, manage) scope.

Step 3: Install and register the Azure Pipelines agent on an Azure virtual machine.

By running a Azure Pipeline agent in the cluster, we make it possible to test any service, regardless of type.

References:

https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-tutorial-deploy-container-app-with-cicd-vsts

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

NEW QUESTION: 206

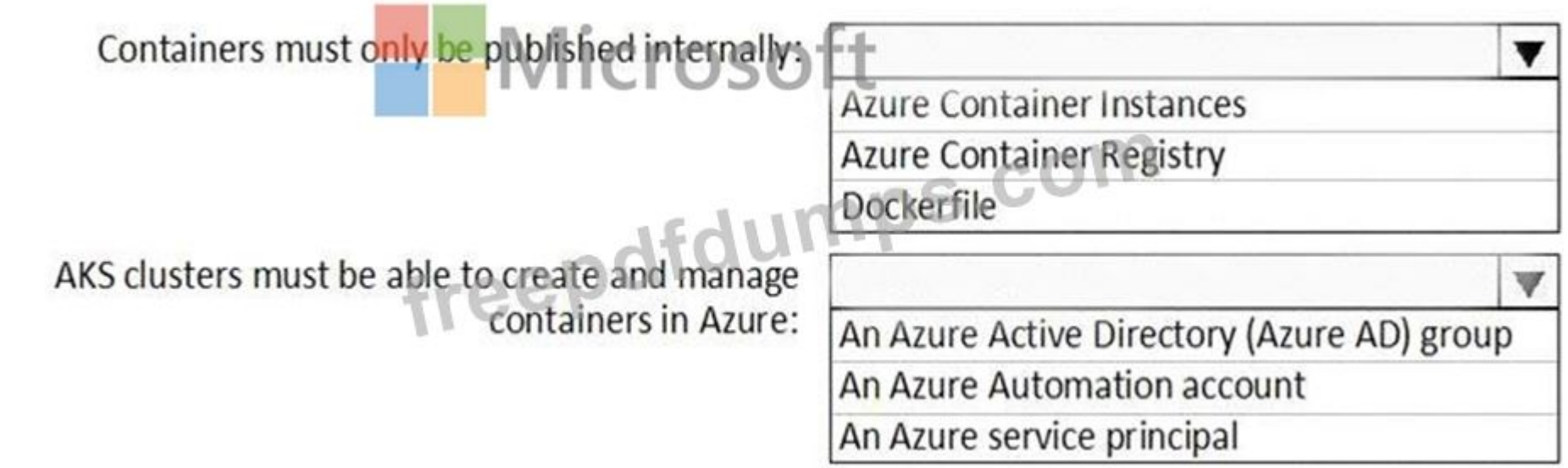
You need to deploy Azure Kubernetes Service (AKS) to host an application. The solution must meet the following requirements:

* Containers must only be published internally.

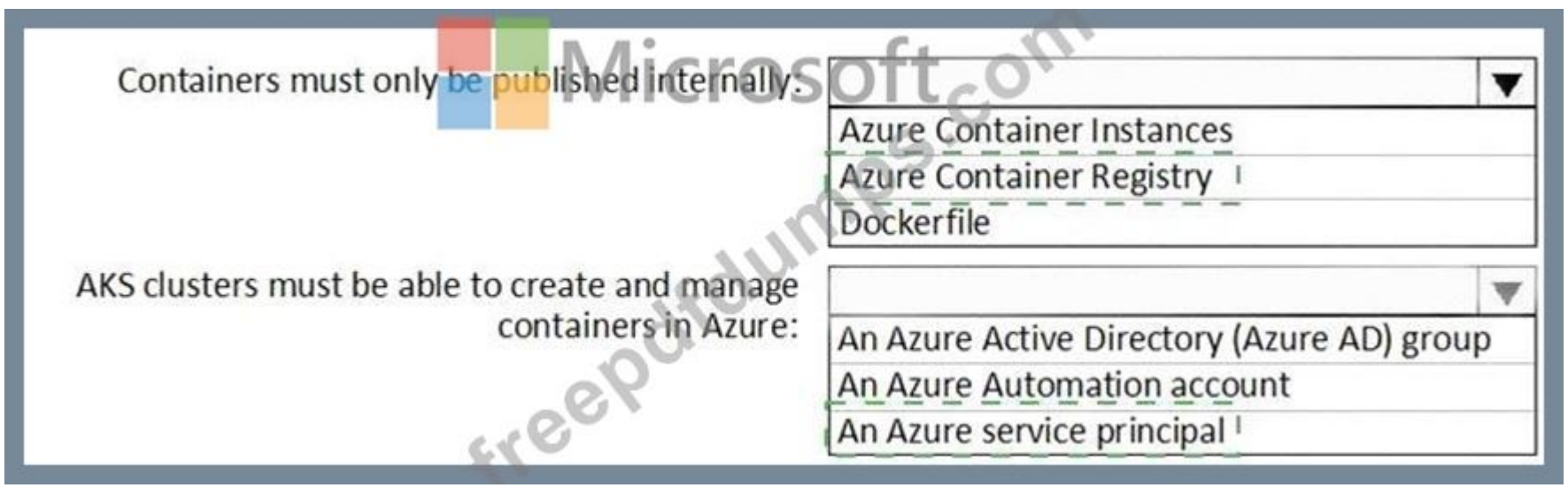
* AKS clusters must be able to create and manage containers in Azure.

What should you use for each requirement? To answer, select the appropriate options in the answer area.

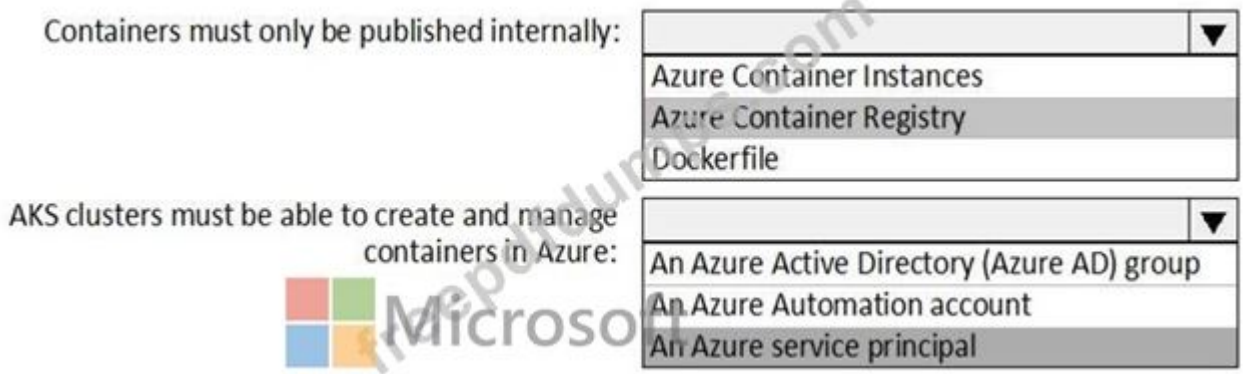
NOTE: Each correct selection is worth one point.



Answer:



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.

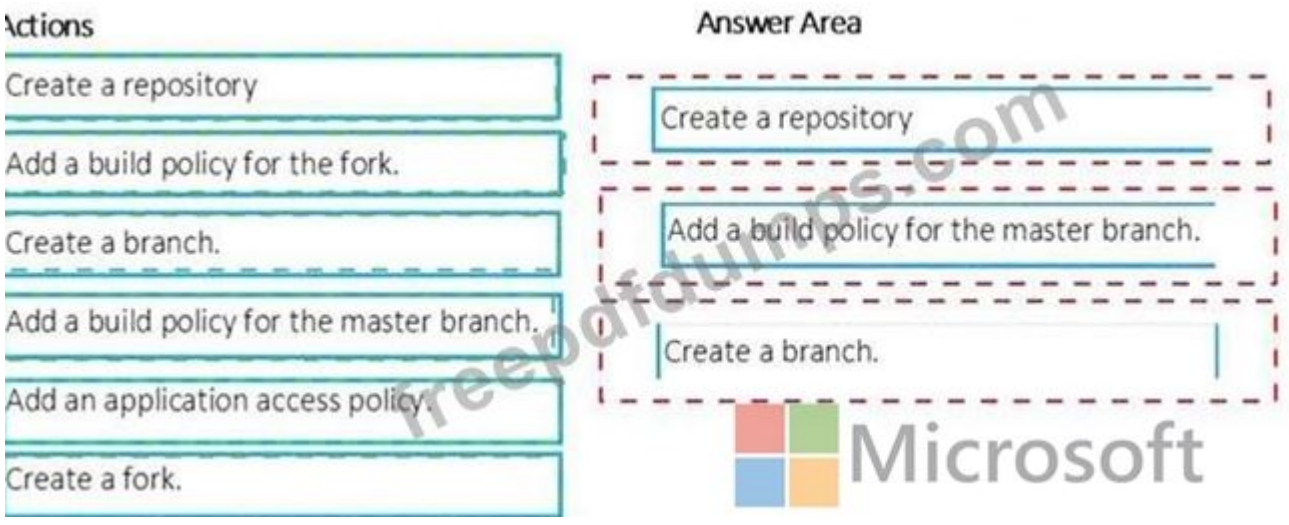
Box 2: An Azure service principal

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

NEW QUESTION: 207
Which package feed access levels should be assigned to the Developers and Team Leaders groups for the investment planning applications suite? To answer, drag the appropriate access levels to the correct groups.
Each access level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Answer:



Explanation

Box 1: Reader

Members of a group named Developers must be able to install packages.
Feeds have four levels of access: Owners, Contributors, Collaborators, and Readers. Owners can add any type of identity-individuals, teams, and

groups-to any access level.
Box 2: Owner
Members of a group named Team Leaders must be able to create new packages and edit the permissions of package feeds.

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

NEW QUESTION: 208
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 Dependency agent
B. the Azure Network Watcher Agent for Windows
C. the Telegraf agent
D. the Azure Log Analytics agent
Answer: (SHOW ANSWER)
The following table provide a quick comparison of the Azure Monitor agents for Windows.

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

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

NEW QUESTION: 209
You need to ensure that an Azure web app named az400-9940427-main can retrieve secrets from an Azure key vault named az400-9940427-kv1 by using a system managed identity.
The solution must use the principle of least privilege.
To complete this task, sign in to the Microsoft Azure portal.
Answer:
See solution below.
Explanation
1. In Azure portal navigate to the az400-9940427-main app.
2. Scroll down to the Settings group in the left navigation.
3. Select Managed identity.

4. Within the System assigned tab, switch Status to On. Click Save.

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

NEW QUESTION: 210
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. build
C. staging
D. production release
Answer: D (LEAVE A REPLY)

NEW QUESTION: 211
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure DevOps project.
Your build process creates several artifacts.

You need to deploy the artifacts to on-premises servers.
Solution: You deploy a Docker build to an on-premises server. You add a Download Build Artifacts task to the deployment pipeline.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
Instead you should deploy an Azure self-hosted agent to an on-premises server.
Note: To build your code or deploy your software using Azure Pipelines, you need at least one agent.
If your on-premises environments do not have connectivity to a Microsoft-hosted agent pool (which is typically the case due to intermediate firewalls), you'll need to manually configure a self-hosted agent on on-premises computer(s).
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops

NEW QUESTION: 212
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.
You need to recommend changes to reduce the accumulated technical debt.
Solution: You recommend increasing the test coverage.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Instead reduce the code complexity.
Note: Technical debt is the accumulation of sub-optimal technical decisions made over the lifetime of an application. Eventually, it gets harder and harder to change things: it's the 'sand in the gears' that sees IT initiatives grind to a halt.
Reference:
https://dzone.com/articles/fight-through-the-pain-how-to-deal-with-technical
https://www.devopsgroup.com/blog/five-ways-devops-helps-with-technical-debt/

NEW QUESTION: 213
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that

might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You plan to create a release pipeline that will deploy Azure resources by using Azure Resource Manager templates. The release pipeline will create the following resources:
* Two resource groups
* Four Azure virtual machines in one resource group
* Two Azure SQL databases in other resource group
You need to recommend a solution to deploy the resources.
Solution: Create a main template that has two linked templates, each of which will deploy the resource in its respective group.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
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

NEW QUESTION: 214
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: (SHOW ANSWER)
Change the ConfigurationMode parameter from ApplyOnly to ApplyAndAutocorrect.
The Register-AzureRmAutomationDscNode cmdlet registers an Azure virtual machine as an APS Desired State Configuration (DSC) node in an Azure Automation account.
Scenario: Current Technical Issue
The test servers are configured correctly when first deployed, but they experience configuration drift over time.
Azure Automation State Configuration fails to correct the configurations.
Azure Automation State Configuration nodes are registered by using the following command.

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

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

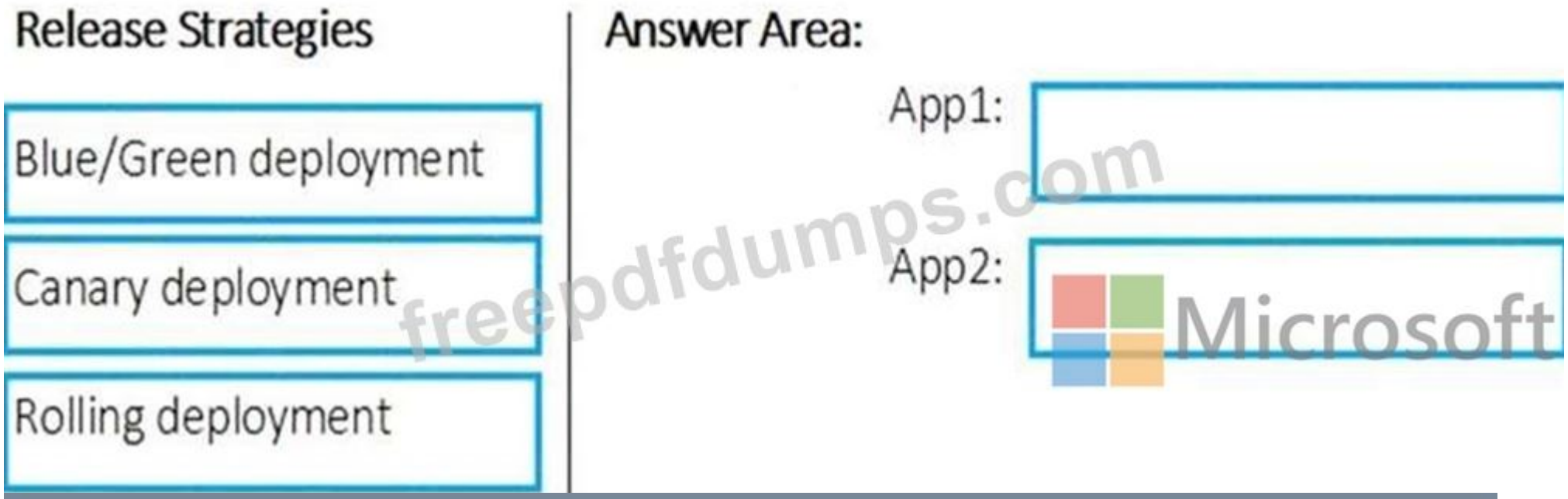
NEW QUESTION: 215

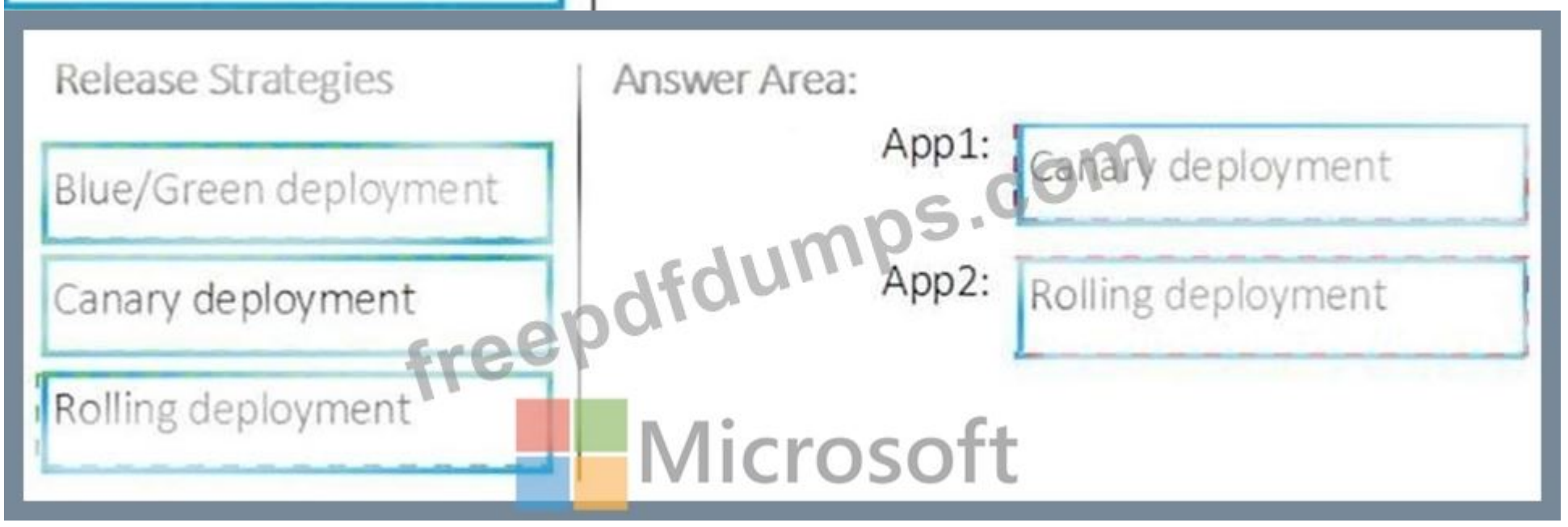
You are defining release strategies for two applications as shown in the following table.

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.





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.

NEW QUESTION: 216
Your company builds a multi tier web application.
>You use Azure DevOps and host the production application on Azure virtual machines.
Your team prepares an Azure Resource Manager template of the virtual machine that you mil use to test new features.
You need to create a staging environment in Azure that meets the following requirements:
* Minimizes the cost of Azure hosting
* Provisions the virtual machines automatically
* Use* the custom Azure Resource Manager template to provision the virtual machines What should you do?
A. In Azure DevOps, configure new tasks in the release pipeline to create and delete the virtual machines m Azure DevTest Labs.
B. From Azure Cloud Shell, run Azure PowerShell commands to create and delete the new virtual machines in a staging resource group.
C. In Azure DevOps, configure new tasks in the release pipeline to deploy to Azure Cloud Services.
D. In Azure Cloud Shell, run Azure CLI commands to create and delete the new virtual machines in a staging resource group.
Answer: A (LEAVE A REPLY)
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

NEW QUESTION: 217
Note: This question is part of * series of questions that present the same scenario. Each question in the series contains a unique solution that

might meet the stated goals. Some question sett might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an approval process that contains a condition. The condition requires that releases be approved by a team leader before they are deployed.
You have a poky stating that approvals must occur within eight hour.
You discover that deployments fail if the approvals take longer than two hours.
You need to ensure that the deployments only fail if the approvals take longer than eight hours.
Solution: From Post-deployment conditions, you modify the Time between re-evaluation of gates option.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Use a gate From Pre-deployment conditions instead.
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates

NEW QUESTION: 218
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 (LEAVE A REPLY)
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
Implement Continuous Feedback
Question Set 1

NEW QUESTION: 219
Your company has an Azure subscription.
The company requires that all resource group in the subscription have a tag named organization set to a value of Contoso.
You need to implement a policy to meet the tagging requirement.
How should you complete the policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
{
 "policyRule": {
   "if": {
     "allOf": [
       {
         "field": "type",
         "equals":
        ,
       {
                                          ▼
                                  "MicrosoftResources/deployments"
                                  "MicrosoftResources/subscriptions"
                                  "MicrosoftResources/subscriptions/resourceGroups"
         "not": {
           "field": "tags['organization']",
           "equals": "Contoso"
         }
       }
     ]
   },

 "then": {
   "effect":                              ▼
                                  "Append",
   "details": [                   "Deny",
                                  "DeployIfNotExists",
     {
       "field": "tags['organization']",
       "value": "Contoso"
     }
   ]
  }
 }
}
```

Answer:

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


Explanation

Box 1: " Microsoft.Resources/subscriptions/resourceGroups"

Box 2: "Deny",

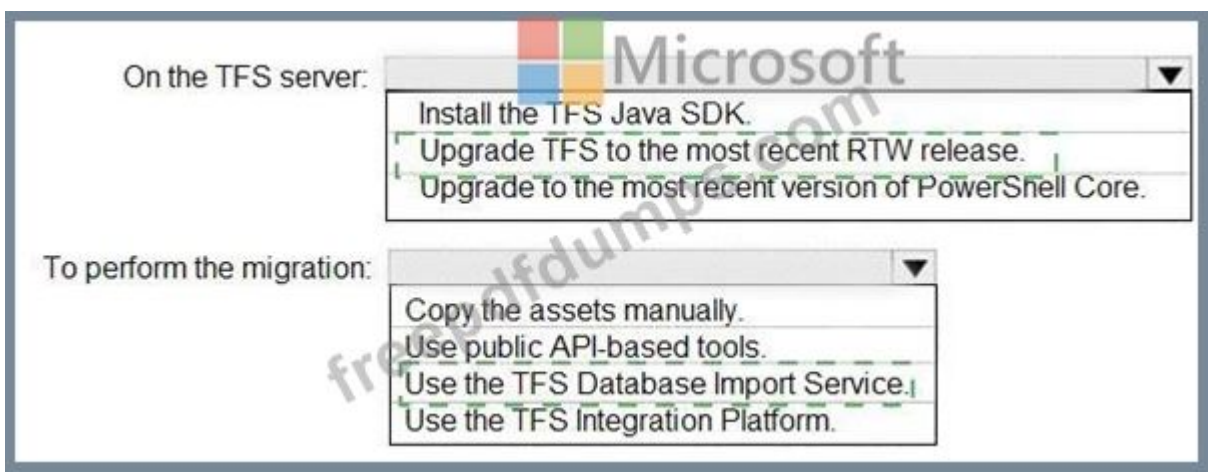
Sample - Enforce tag and its value on resource groups

```
},
"policyRule": {
"if": {
"allOf": [
{
"field": "type",
"equals": "Microsoft.Resources/subscriptions/resourceGroups"
},
{
"not": {
"field": "[concat('tags[',parameters('tagName'), ']')]",
"equals": "[parameters('tagValue')]"
}
}
]
},
```

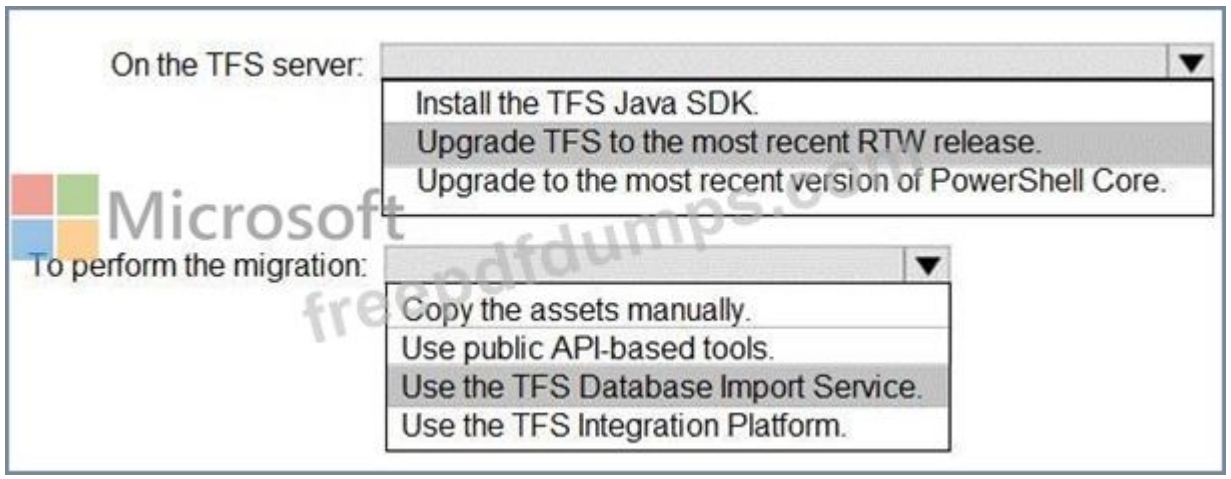
"then": {
"effect": "deny"
}
}
}
}
References:
https://docs.microsoft.com/en-us/azure/governance/policy/samples/enforce-tag-on-resource-groups

NEW QUESTION: 220
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.

Answer:



Explanation



Box 1: Upgrade TFS to the most recent RTM release.

One of the major prerequisites for migrating your Team Foundation Server database is to get your database schema version as close as possible to what is currently deployed in Azure Devops Services.

Box 2: Use the TFS Database Import Service

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

References: Team Foundation Server to Azure Devops Services Migration Guide

NEW QUESTION: 221

HOTSPOT

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

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

Which resource type should you use for each deployment? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Deployment 1:

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

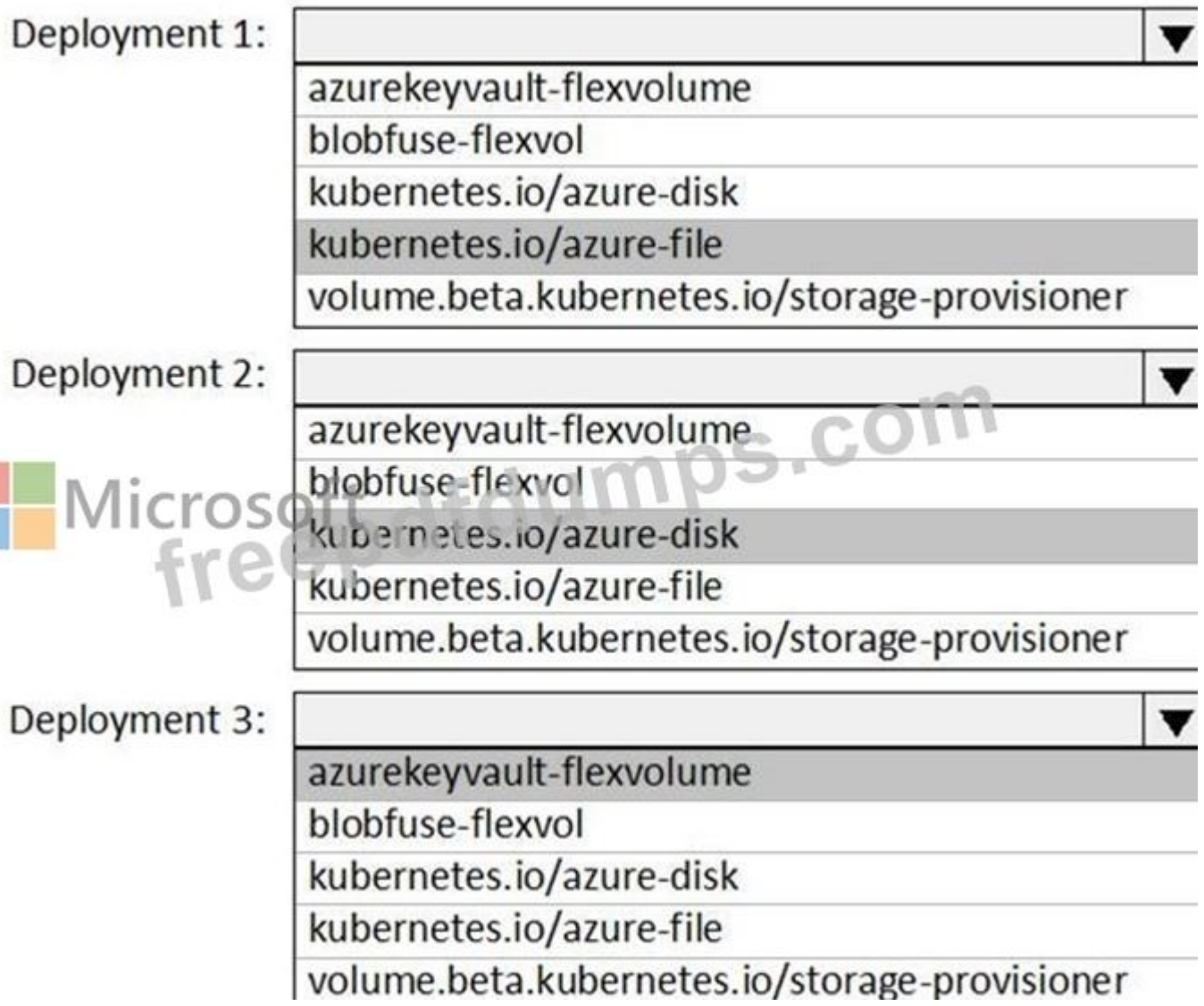
Deployment 2:

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

Deployment 3:

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

Answer:



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.

NEW QUESTION: 222
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.

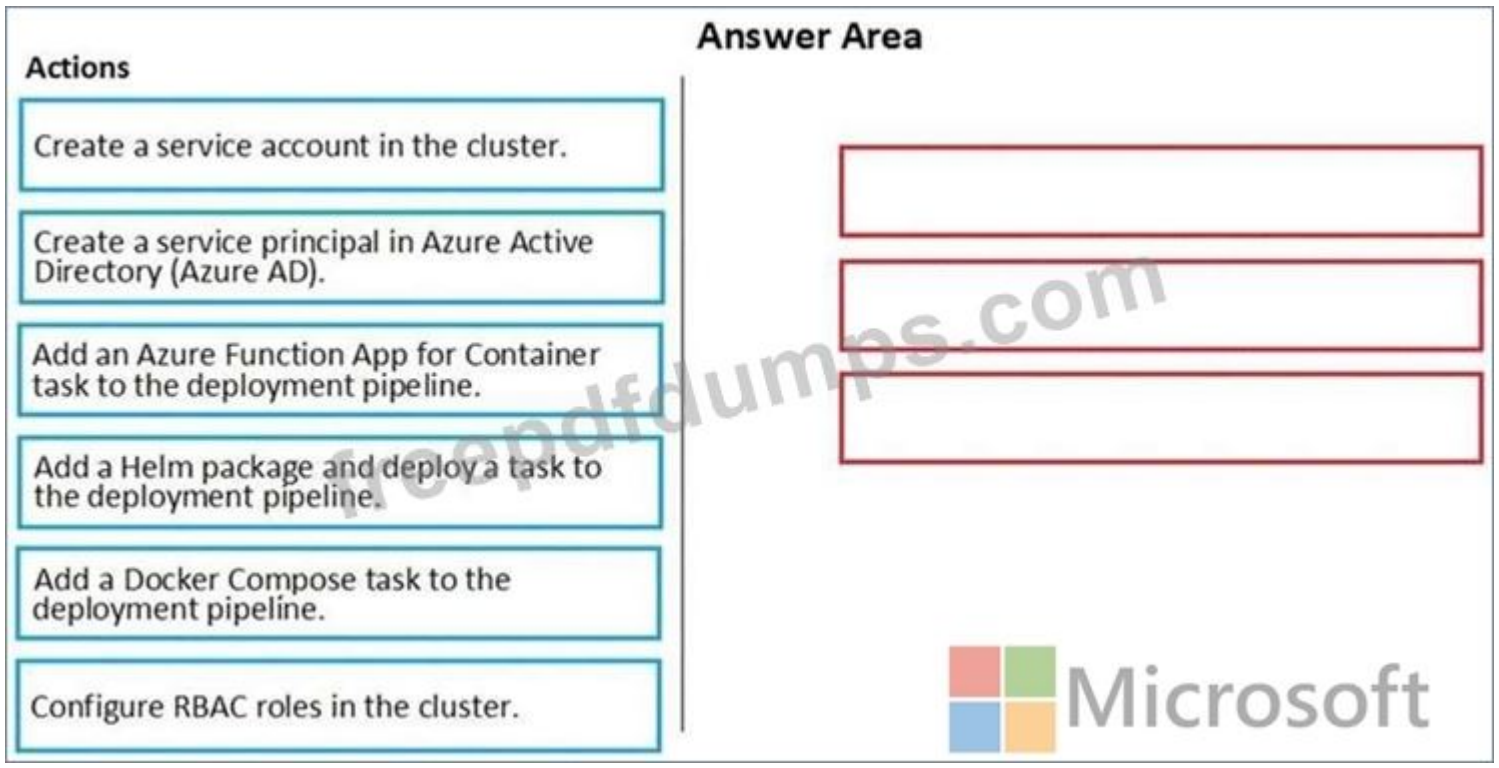
Answer: B (LEAVE A REPLY)
For containerized applications that serve traffic, you might want to verify that your container is ready to handle incoming requests. Azure Container Instances supports readiness probes to include configurations so that your container can't be accessed under certain conditions.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

NEW QUESTION: 223
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a project in Azure DevOps for a new web application.
You need to ensure that when code is checked in, a build runs automatically.
Solution: From the Continuous deployment trigger settings of the release pipeline, you enable the Pull request trigger setting.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Explanation/Reference:
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

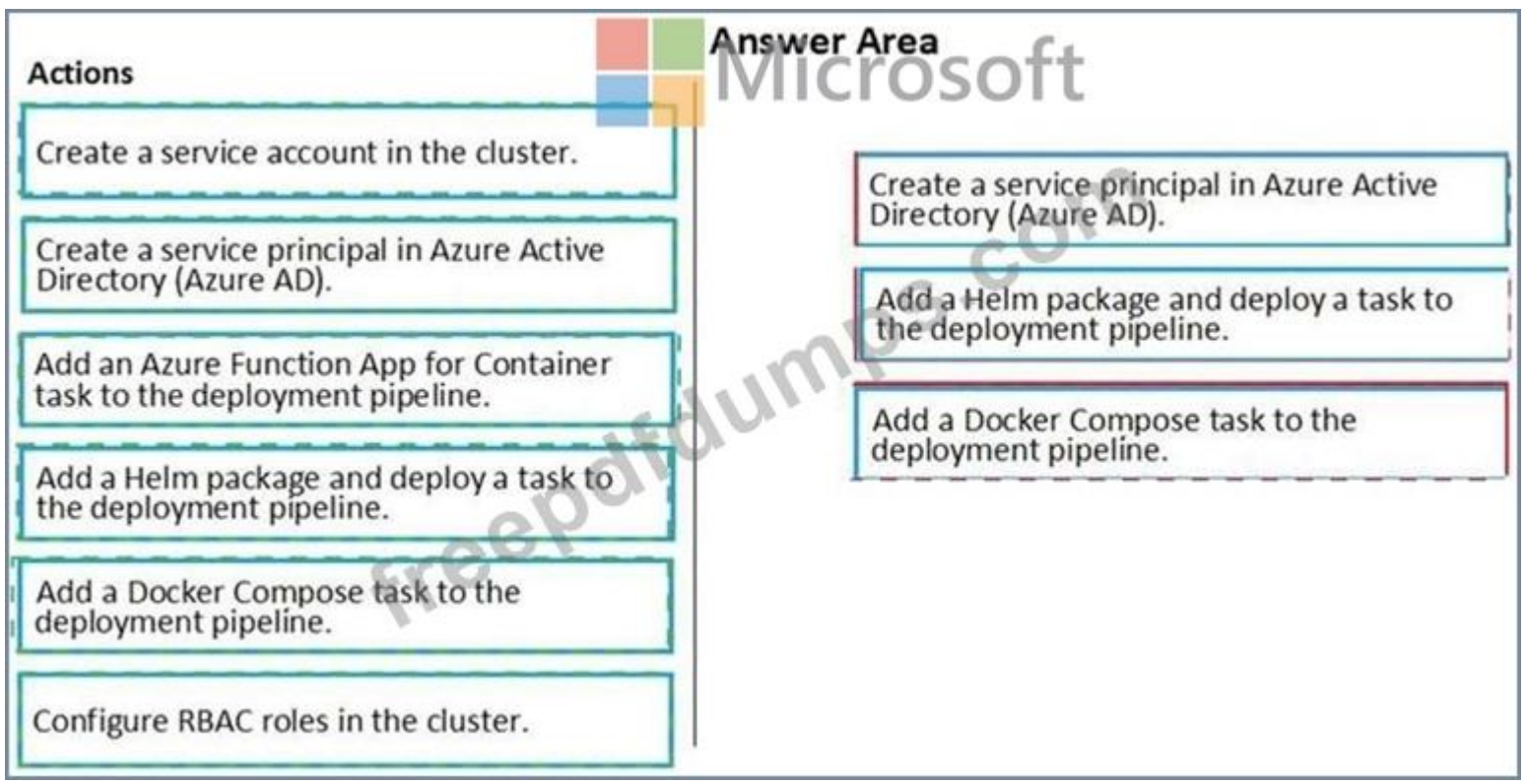
NEW QUESTION: 224
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a prefect in Azure DevOps for a new web application.
You need to ensure that when code is checked in, a build runs automatically.
Solution: from the Triggers tab of the build pipeline, you select Enable continuous integration
Does the meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/get-started-designer

NEW QUESTION: 225
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: A,B,E (LEAVE A REPLY)
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

NEW QUESTION: 226
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



Answer:



Explanation

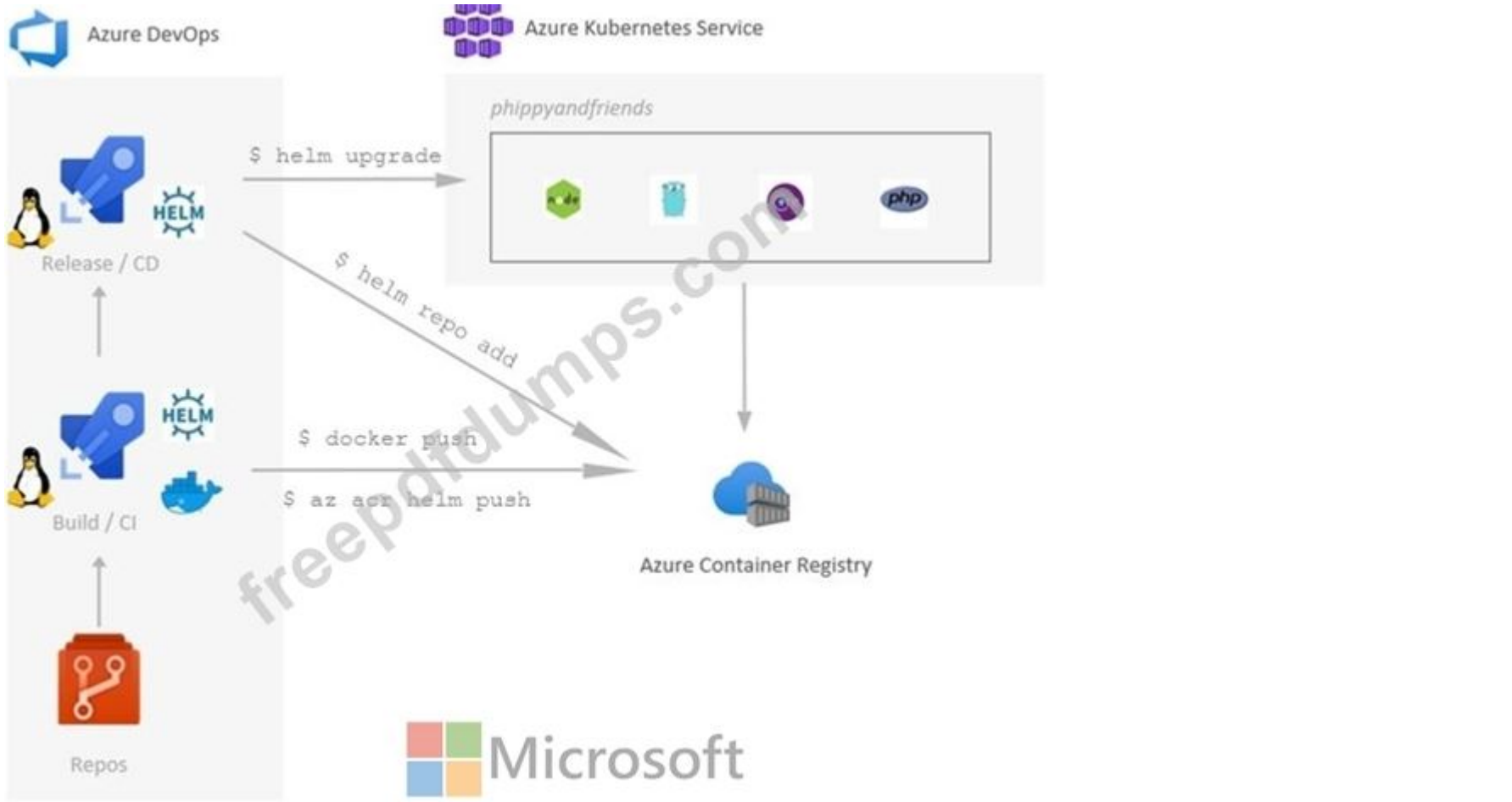
You can set up a CI/CD pipeline to deploy your apps on a Kubernetes cluster with Azure DevOps by leveraging a Linux agent, Docker, and Helm.

Step 1: Create a service principle in Azure Active Directory (Azure AD) We need to assign 3 specific service principals with specific Azure Roles that need to interact with our ACR and our AKS.

Create a specific Service Principal for our Azure DevOps pipelines to be able to push and pull images and charts of our ACR.

Create a specific Service Principal for our Azure DevOps pipelines to be able to deploy our application in our AKS.

Step 2: Add a Helm package and deploy a task to the deployment pipeline This is the DevOps workflow with containers:



Step 3: Add a Docker Compose task to the deployment pipeline.

Dockerfile file is a script leveraged by Docker, composed of various commands (instructions) and arguments listed successively to automatically perform actions on a base image in order to create a new Docker image by packaging the app.

Reference:

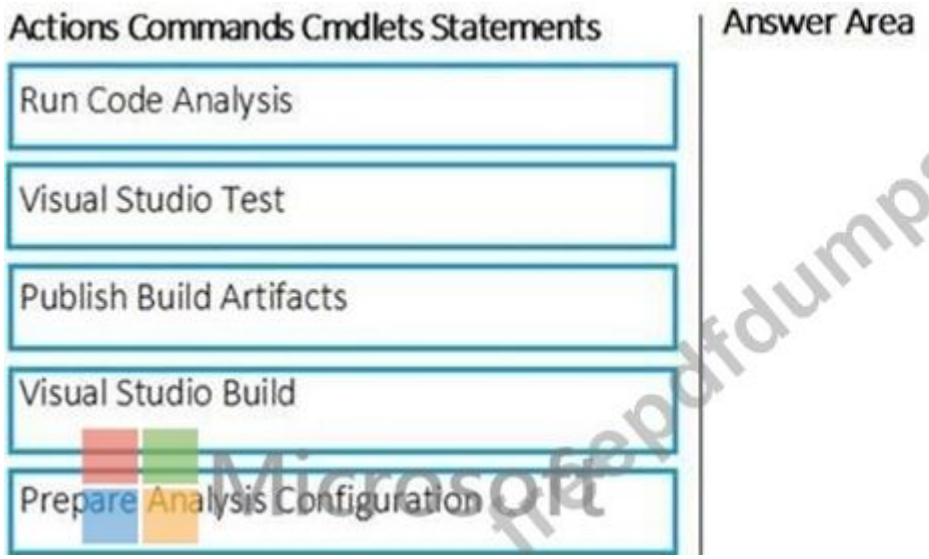
https://cloudblogs.microsoft.com/opensource/2018/11/27/tutorial-azure-devops-setup-cicd-pipeline-kubernetes-d

NEW QUESTION: 227
During a code review, you discover quality issues in a Java application.
You need to recommend a solution to detect quality issues including unused variables and empty catch blocks.
What should you recommend?
A. In a Maven build task, select Run PMD.
B. In a Grunt build task, select Enabled from Control Options.
C. In an Xcode build task, select Use xcpretty from Advanced.
D. In a Gulp build task, specify a custom condition expression.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 228
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You plan to update the Azure DevOps strategy of your company.
You need to identify the following issues as they occur during the company's development process:
* Licensing violations
* Prohibited libraries
Solution: You implement pre-deployment gates.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
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 denitive database of open source repositories.
Reference:
https://azuredevopslabs.com/labs/vstsextend/whitesource/

NEW QUESTION: 229
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.
DRAG DROP
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.



Answer:

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:

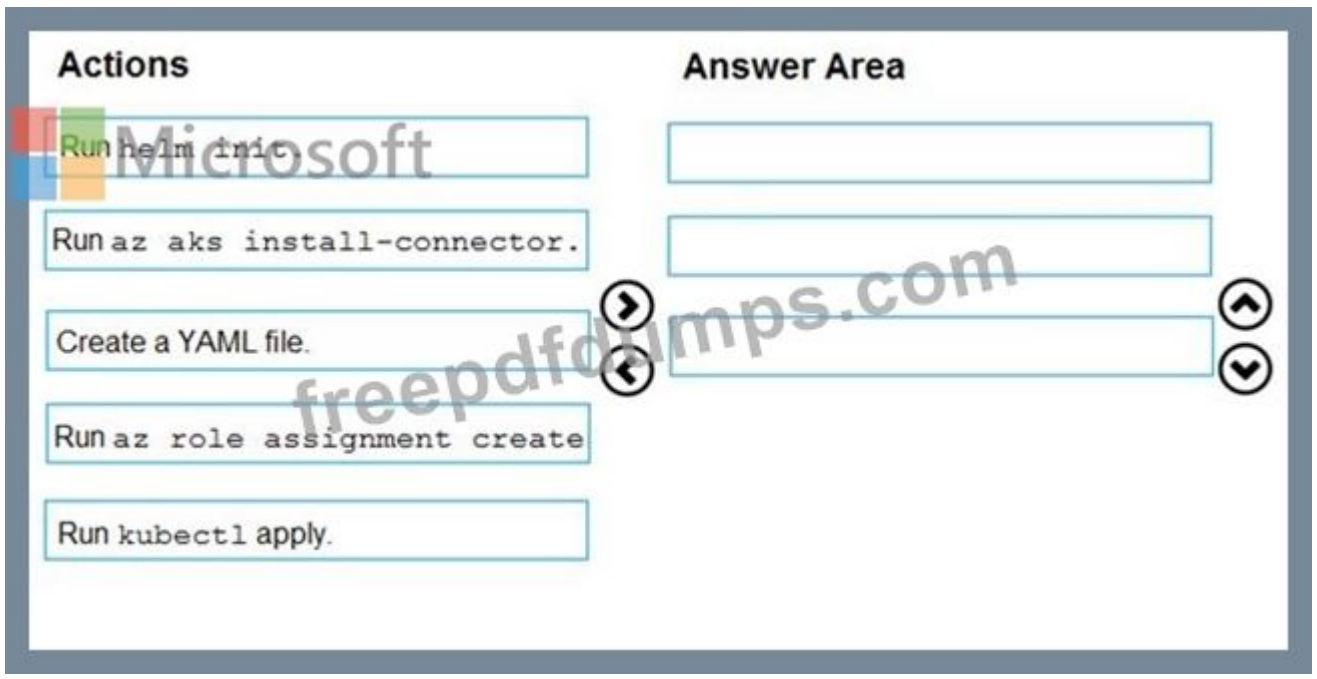
Prepare Analysis Configuration task before any MSBuild or Visual Studio Build task.

Step 3: Visual Studio Test

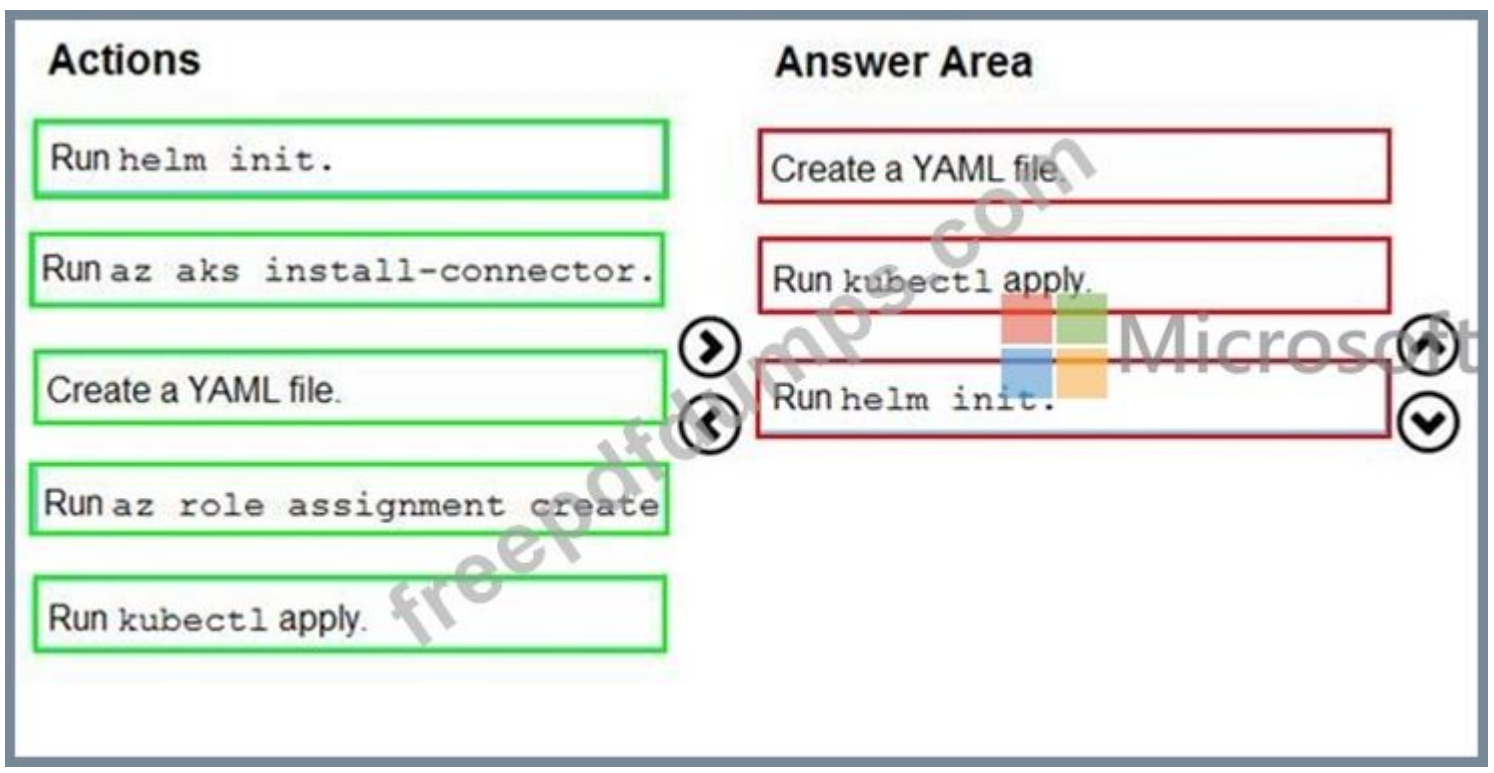
Reorder the tasks to respect the following order:
Run Code Analysis task after the Visual Studio Test task.
Step 4: Run Code Analysis
Run Code Analysis task, to actually execute the analysis of the source code.
This task is not required for Maven or Gradle projects, because scanner will be run as part of the Maven/Gradle build.
Note:

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

NEW QUESTION: 230
You have an Azure Kubermets Service (AKS) implementation that is RBAC-enabled
You plan to use Azure Container Instances as a hosted development environment to run containers in the AKS implementation.
You need to conjure Azure Container Instances as a hosted environment for running me containers in AKS. Which three actions should you perform m sequence?
To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:

Step 1: Create a YAML file.

If your AKS cluster is RBAC-enabled, you must create a service account and role binding for use with Tiller. To create a service account and role binding, create a file named rbac-virtual-kubelet.yaml

Step 2: Run kubectl apply.

Apply the service account and binding with kubectl apply and specify your rbac-virtual-kubelet.yaml file.

Step 3: Run helm init.

Configure Helm to use the tiller service account:

helm init --service-account tiller

You can now continue to installing the Virtual Kubelet into your AKS cluster.

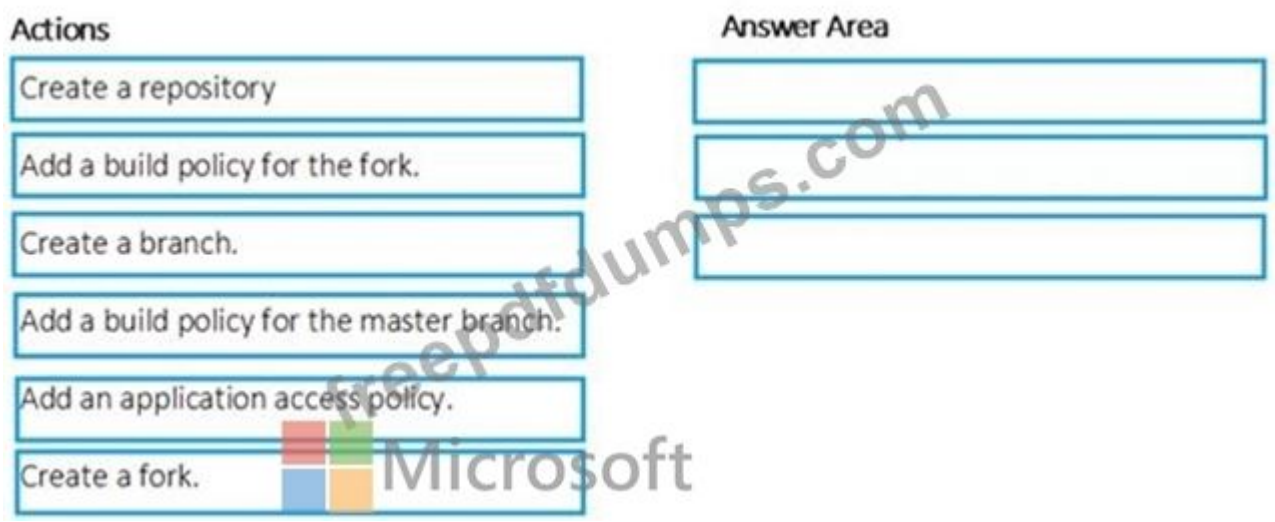
References:
https://docs.microsoft.com/en-us/azure/aks/virtual-kubelet

NEW QUESTION: 231
You manage the Git repository for a large enterprise application.
You need to minimize the data size of the repository.
How should you complete the commands? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

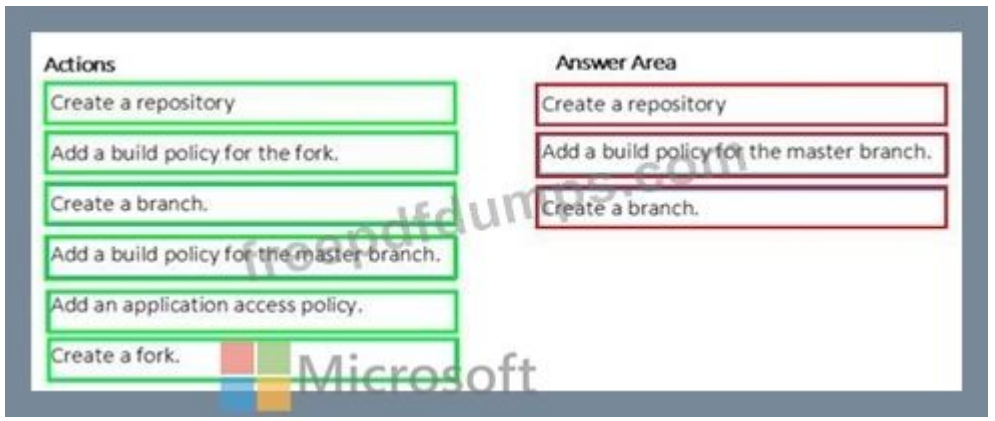
Answer:

Explanation

NEW QUESTION: 232
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.



Answer:

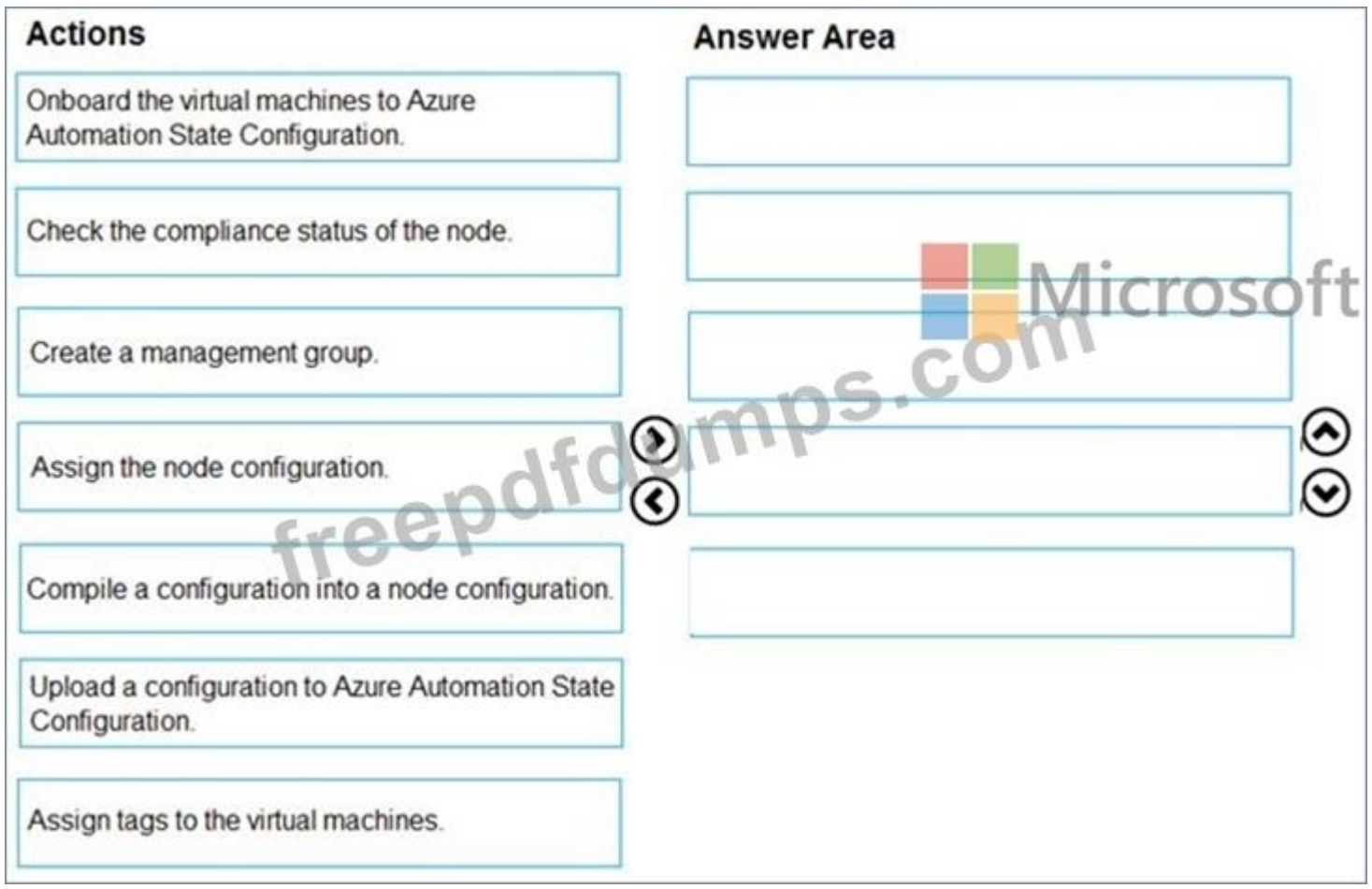


NEW QUESTION: 233

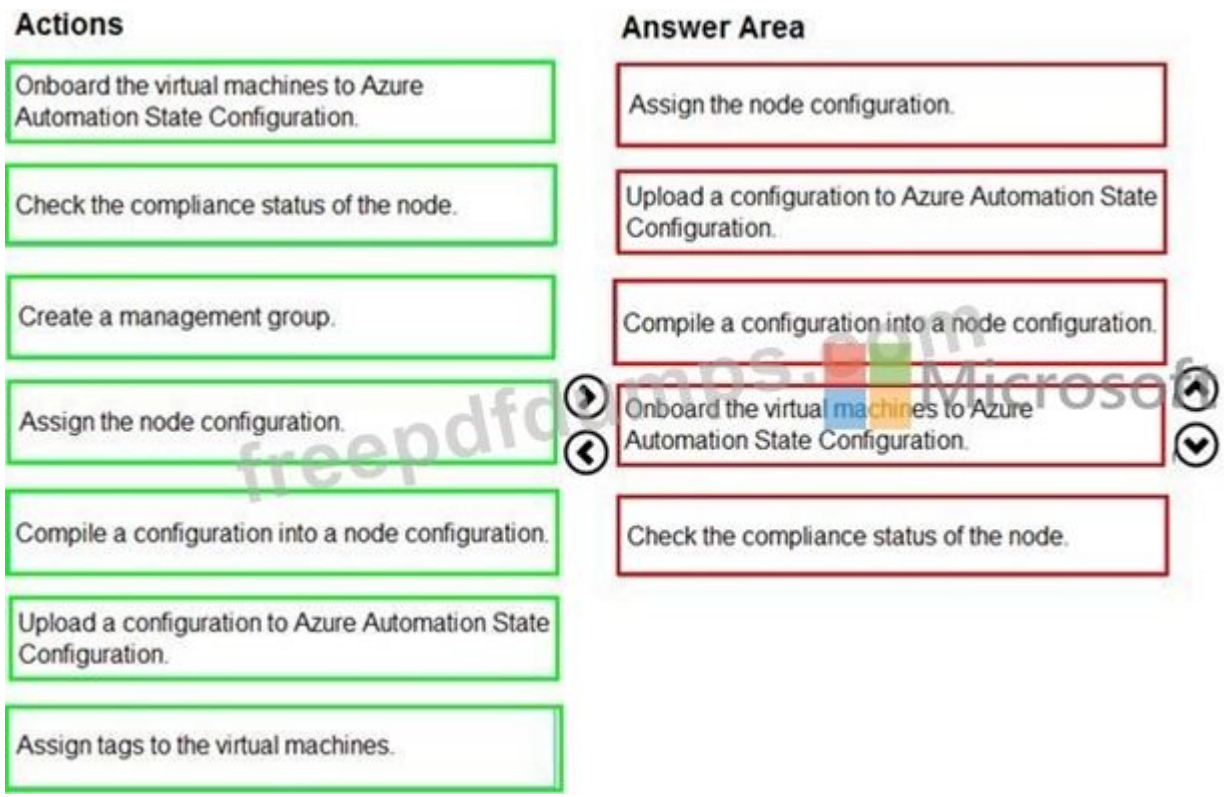
You need to use Azure Automation Sure Configuration to manage the ongoing consistency of virtual machine configurations.

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

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



Answer:



Explanation:

Step 1: Assign the node configuration.

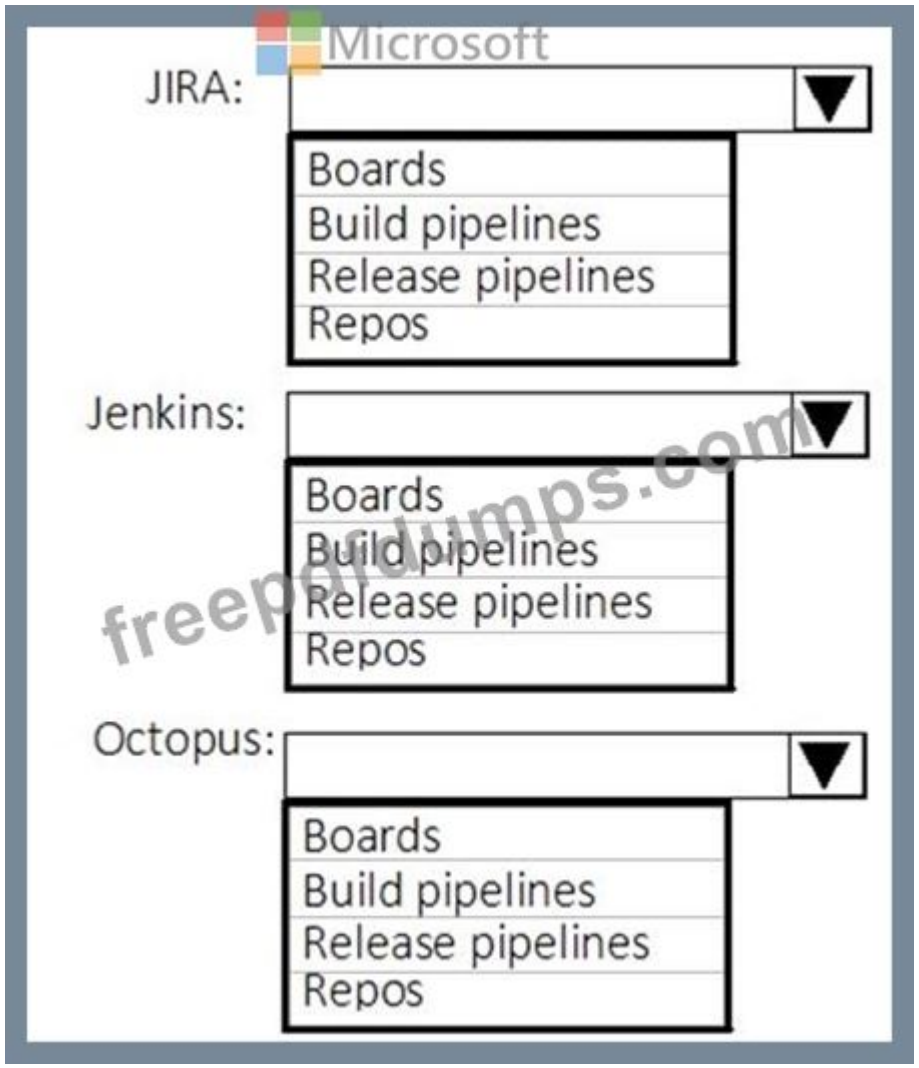
You create a simple DSC configuration that ensures either the presence or absence of the Web-Server Windows Feature (IIS), depending on how you assign nodes.

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

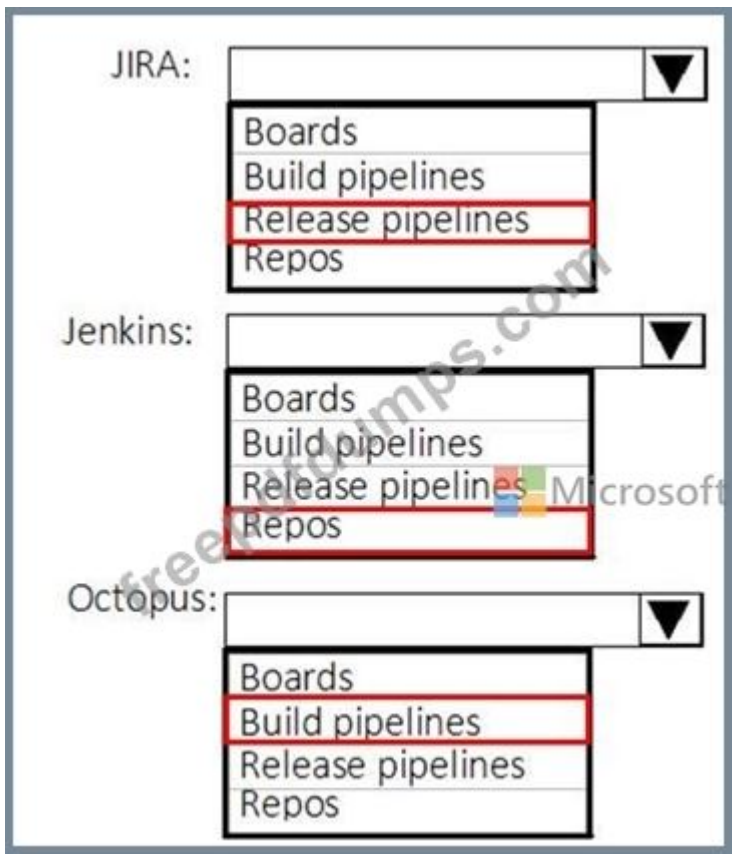
NEW QUESTION: 234
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You plan to update the Azure DevOps strategy of your company.
You need to identify the following issues as they occur during the company's development process:
* Licensing violations
* Prohibited libraries
Solution: You implement continuous integration.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
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/

NEW QUESTION: 235
You currently use JIRA, Jenkins, and Octopus as part of your DevOps processes.
You plan to use Azure DevOps to replace these tools.
Which Azure DevOps service should you use to replace each tool? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



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/

NEW QUESTION: 236

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 self-hosted agent.

You need to implement the self-hosted agent.

You download and install the agent on the build server.

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

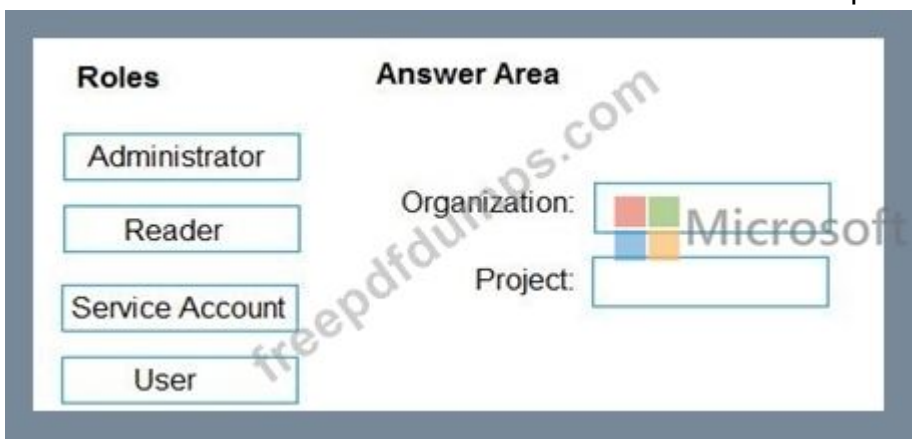
A. From Azure, create a shared access signature (SAS).

B. From the build server, create a certificate, and then upload the certificate to Azure Storage.

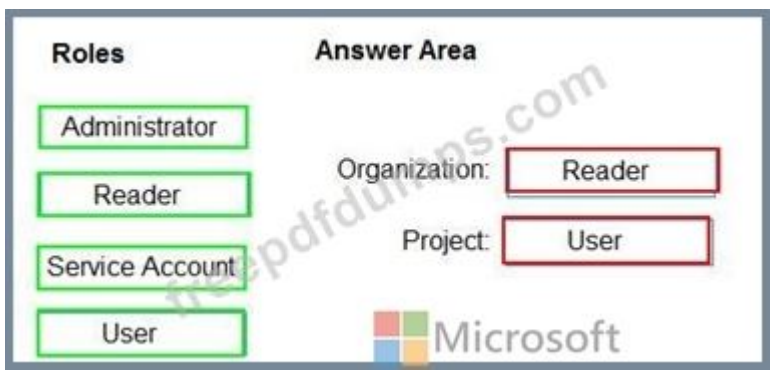
C. From the build server, create a certificate, and then upload the certificate to Azure Key Vault.

D. From DevOps, create a personal access token (PAT).
E. From the build server, run config.cmd.
Answer: D,E (LEAVE A REPLY)
Explanation
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-windows?view=azure-devops (Get PAT, run config)

NEW QUESTION: 237
You need to configure access to Azure DevOps Agent pools to meet the forwarding requirements:
* Use a project agent pool when authoring build release pipelines.
* View the agent pool and agents of the organization.
* Use the principle of least privilege.
Which role memberships are required for the Azure 0e%Oos organization and the project? To answer, drag the appropriate role membership to the correct targets. Each role membership may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to content NOTE: Each correct selection is worth one point.

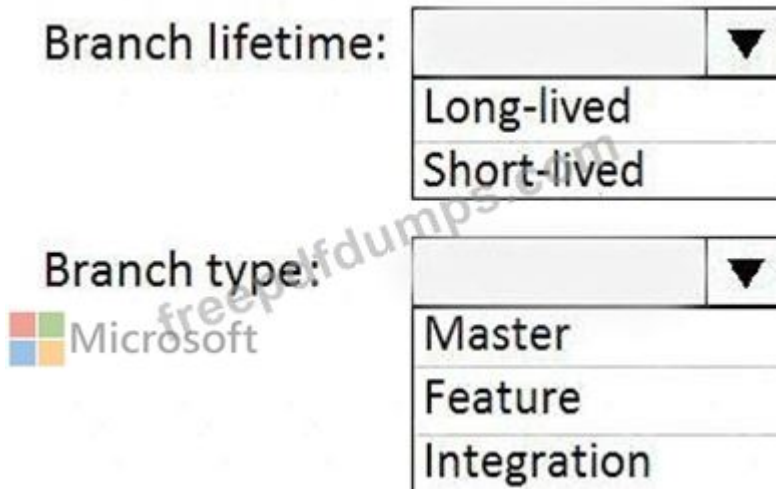


Answer:

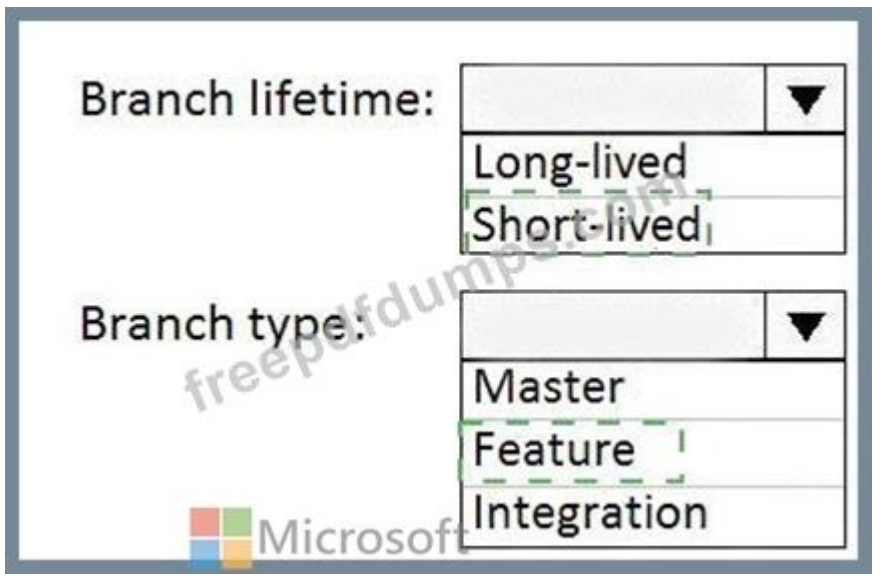


Explanation:
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues

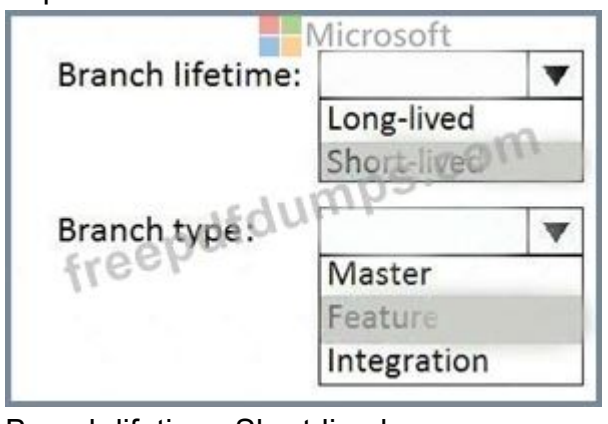
NEW QUESTION: 238
Your company uses Git as a source code control system for a complex app named App1.
You plan to add a new functionality to App1.
You need to design a branching model for the new functionality.
Which branch lifetime and branch time should you use in the branching model? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation



Branch lifetime: Short-lived

Branch type: Feature

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

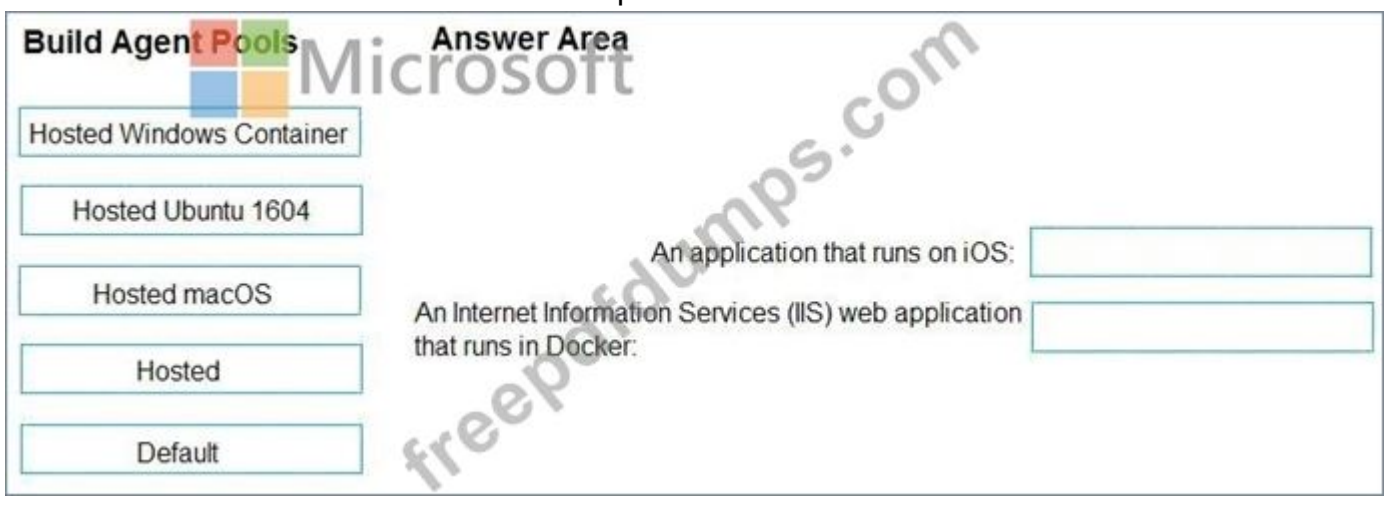
References:

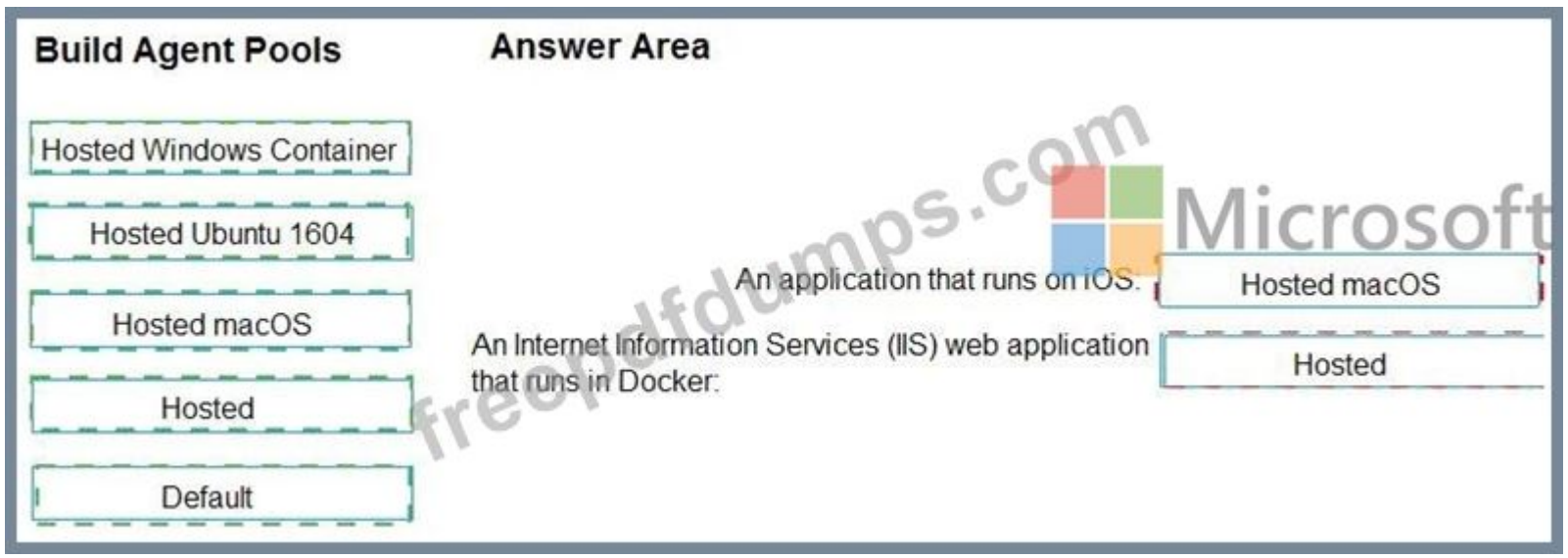
https://gist.github.com/digitaljhelms/4287848

NEW QUESTION: 239

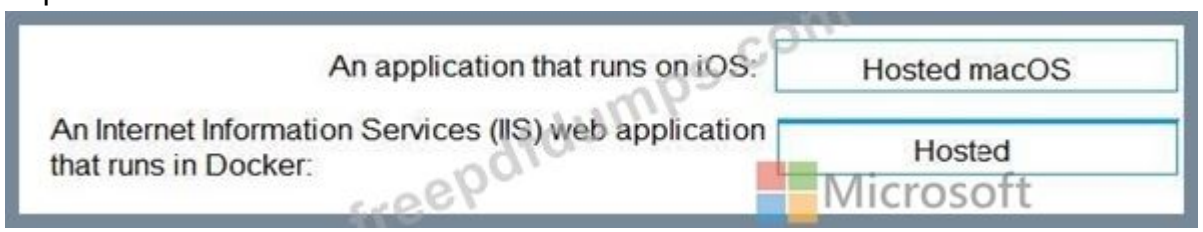
You are designing a build pipeline in Azure Pipelines.
The pipeline requires a self-hosted agent. The build pipeline will run once daily and will take 30 minutes to complete.
You need to recommend a compute type for the agent. The solution must minimize costs.
What should you recommend?
A. an Azure Kubernetes Service (AKS) cluster
B. Azure Container Instances
C. an Azure virtual machine scale set
D. Azure virtual machines
Answer: B (LEAVE A REPLY)
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

NEW QUESTION: 240
You mc configuring Azure DevOps build pipelines.
You plan to use hosted build agents.
Which build agent pool should you use to compile each application type? To answer, drag the appropriate built agent pools to the correct application types. Each butt agent pool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.





Explanation



Box 1: Hosted macOS

Hosted macOS pool (Azure Pipelines only): Enables you to build and release on macOS without having to configure a self-hosted macOS agent. This option affects where your data is stored.

Box 2: Hosted

Hosted pool (Azure Pipelines only): The Hosted pool is the built-in pool that is a collection of Microsoft-hosted agents.

NEW QUESTION: 241

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a project in Azure DevOps.
You need to prevent the configuration of the project from changing over time.
Solution: Perform a Subscription Health scan when packages are created.
Does this meet the goal?

A. Yes

B. No

Answer: (SHOW ANSWER)

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

NEW QUESTION: 242
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.
You need to recommend changes to reduce the accumulated technical debt.
Solution: You recommend increasing the code duplication.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
Explanation
Instead reduce the code complexity.
Reference:
https://dzone.com/articles/fight-through-the-pain-how-to-deal-with-technical

NEW QUESTION: 243
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an approval process that contains a condition. The condition requires that releases be approved by a team leader before they are deployed.
You have a policy stating that approvals must occur within eight hours.
You discover that deployment fail if the approvals take longer than two hours.
You need to ensure that the deployments only fail if the approvals take longer than eight hours.
Solution: From Pre-deployment conditions, you modify the Timeout setting for pre-deployment approvals.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Use a gate instead of an approval instead.
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates

NEW QUESTION: 244
You plan to deploy a runbook that will create Azure AD user accounts.
You need to ensure that runbooks can run the Azure PowerShell cmdlets for Azure Active Directory.
To complete this task, sign in to the Microsoft Azure portal.
A. Azure Automation now ships with the Azure PowerShell module of version 0.8.6, which introduced the ability to non-interactively authenticate to Azure using OrgId (Azure Active Directory user) credential-based authentication. Using the steps below, you can set up Azure Automation to talk to Azure using this authentication type.
Step 1: Find the Azure Active Directory associated with the Azure subscription to manage:
1. Log in to the Azure portal as the service administrator for the Azure subscription you want to manage using Azure Automation. You can find this user by logging in to the Azure portal as any user with access to this Azure subscription, then clicking Settings, then Administrators.

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

Step 2: Create an Azure Active Directory user in the directory associated with the Azure subscription to manage:
You can skip this step if you already have an Azure Active Directory user in this directory. and plan to use this OrgId to manage Azure.

ve Directory service.

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

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

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

2. Click Administrators

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

Step 4: Configure Azure Automation to use this Azure Active Directory user to manage this Azure subscription Create an Azure Automation credential asset containing the username and password of the Azure Active Directory user that you have just created. You can create a credential asset in Azure Automation by clicking into an Automation Account and then clicking the Assets tab, then the Add Setting button.

Note: Once you have set up the Azure Active Directory credential in Azure and Azure Automation, you can now manage Azure from Azure Automation runbooks using this credential.

B. Azure Automation now ships with the Azure PowerShell module of version 0.8.6, which introduced the ability to non-interactively authenticate to Azure using OrgId (Azure Active Directory user) credential-based authentication. Using the steps below, you can set up Azure Automation to talk to Azure using this authentication type.

Step 1: Find the Azure Active Directory associated with the Azure subscription to manage:

1. Log in to the Azure portal as the service administrator for the Azure subscription you want to manage using Azure Automation. You can find

this user by logging in to the Azure portal as any user with access to this Azure subscription, then clicking Settings, then Administrators.

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

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

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

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

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

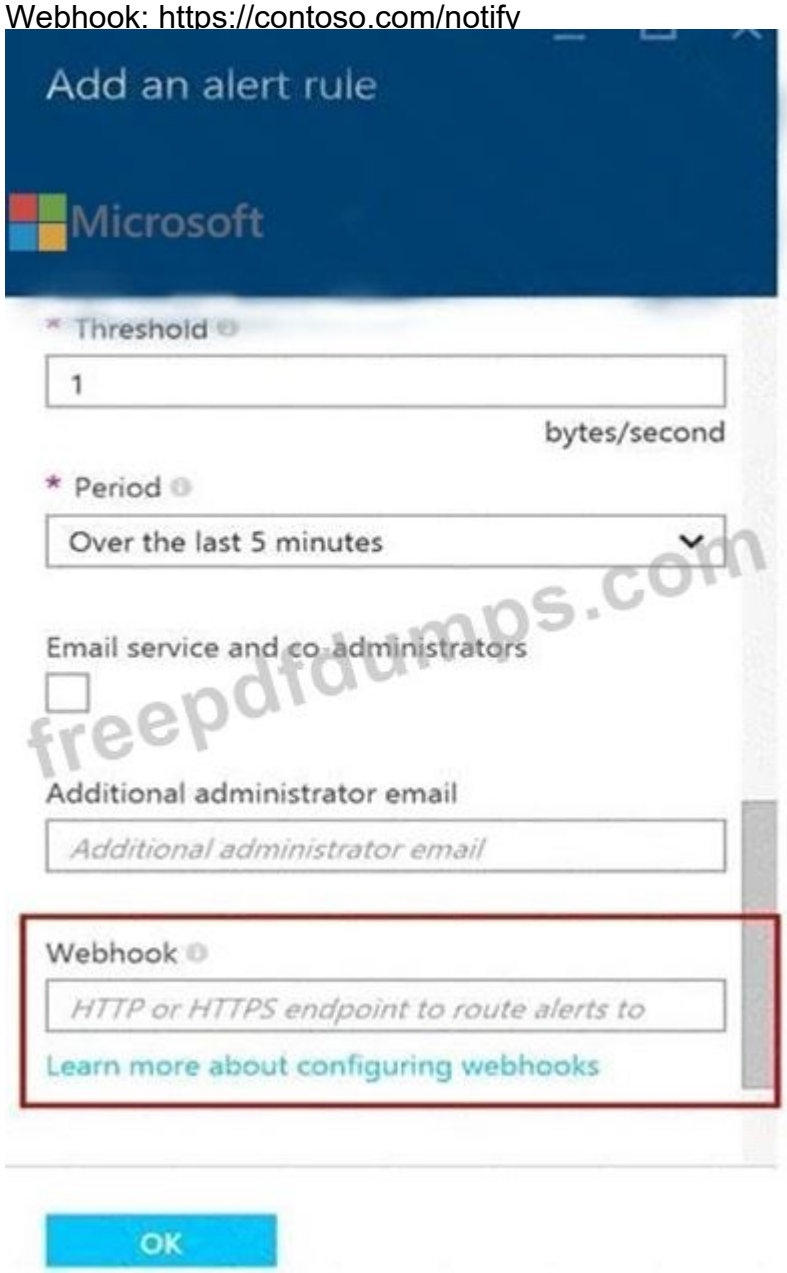
1. Click on Settings (bottom Azure tab under StorSimple)

2. Click Administrators
3. Click the Add button. Type the full user name (including part after @ symbol) of the Azure Active Directory user you want to set up to manage Azure. For subscriptions, choose the Azure subscriptions you want this user to be able to manage. Click the check mark.
Step 4: Configure Azure Automation to use this Azure Active Directory user to manage this Azure subscription Create an Azure Automation credential asset containing the username and password of the Azure Active Directory user that you have just created. You can create a credential asset in Azure Automation by clicking into an Automation Account and then clicking the Assets tab, then the Add Setting button.

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

NEW QUESTION: 245
You need to create a notification if the peak average response time of an Azure web app named az400-9940427-main is more than five seconds when evaluated during a five-minute period. The notification must trigger the "https://contoso.com/notify" webhook.
To complete this task, sign in to the Microsoft Azure portal.
Answer:
See solution below.
Explanation
1. Open Microsoft Azure Portal
2. Log into your Azure account and go to App Service and look under Monitoring then you will see Alert.
3. Select Add an alert rule
4. Configure the alert rule as per below and click Ok.
Source: Alert on Metrics
Resource Group: az400-9940427-main
Resource: az400-9940427-main
Threshold: 5

Period: Over the last 5 minutes
Webhook: https://contoso.com/notify

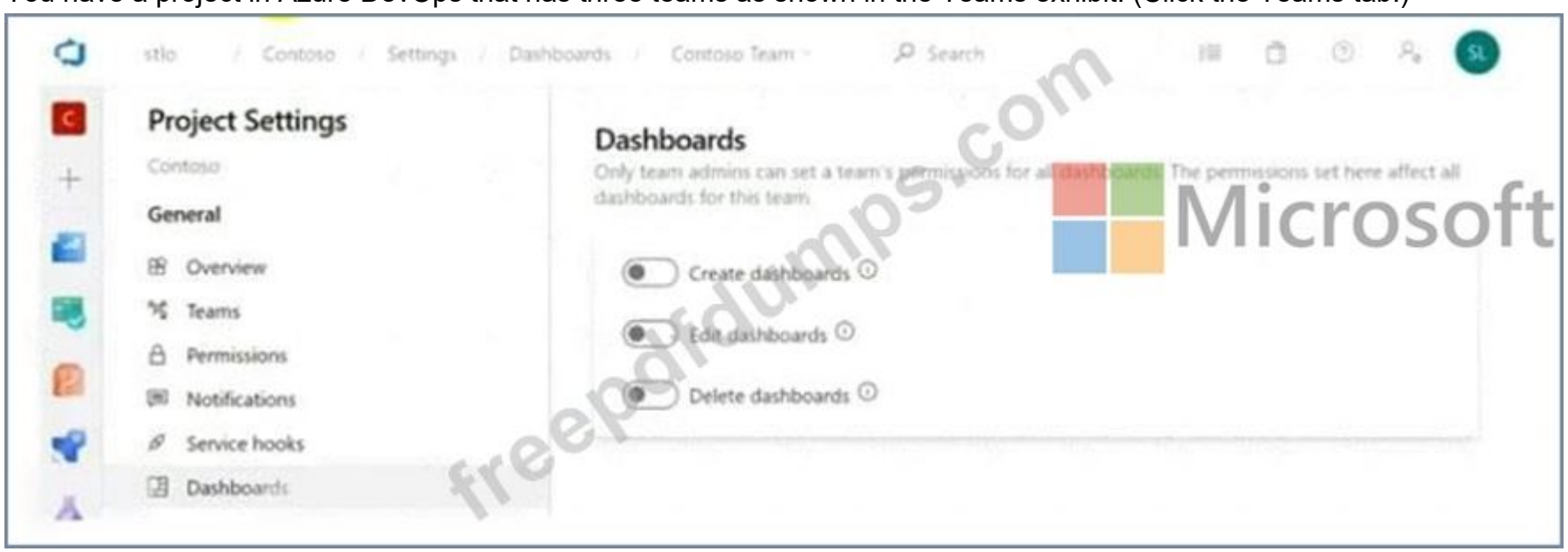


References:
https://azure.microsoft.com/es-es/blog/webhooks-for-azure-alerts/

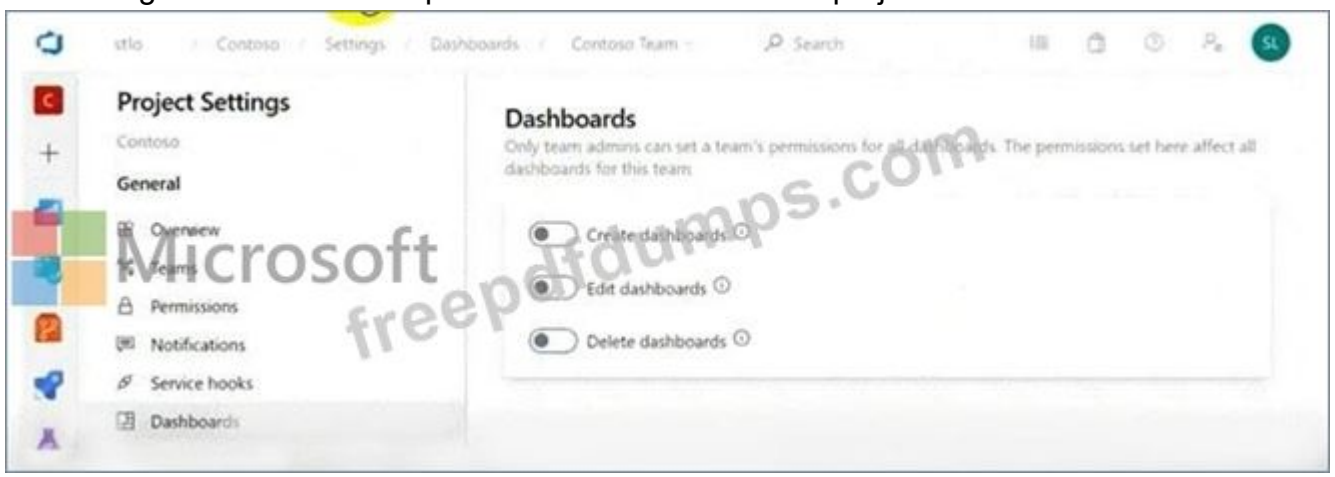
NEW QUESTION: 246
You have an Azure Resource Manager template that deploys a multi-tier application.
You need to prevent the user who performs the deployment from viewing the account credentials and connection strings used by the application.
What should you use?
A. Azure Key Vault
B. a Web.config file
C. an Appsettings.json file
D. an Azure Storage table
E. an Azure Resource Manager parameter file
Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 247
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 Contoso project as shown in the Permissions exhibit (Click the Permissions tab.)



All other permissions have the default values set.

Answer:

Explanation

NEW QUESTION: 248

Your company has a project in Azure DevOps for a new web application.

The company identifies security as one of the highest priorities.

You need to recommend a solution to minimize the likelihood that infrastructure credentials will be leaked.

What should you recommend?

A. Add a Run Inline Azure PowerShell task to the pipeline.

B. Add a PowerShell task to the pipeline and run Set-AzureKeyVaultSecret.

C. Add a Azurre Key Vault task to the pipeline.

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 249

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:

Explanation:

Box 1: Azure Pipelines service connection

Box 2: Managed Service Identity Authentication

The managed identities for Azure resources feature in Azure Active Directory (Azure AD) provides Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code.

Reference:

https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/deploy/azure-key-vault

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

NEW QUESTION: 250

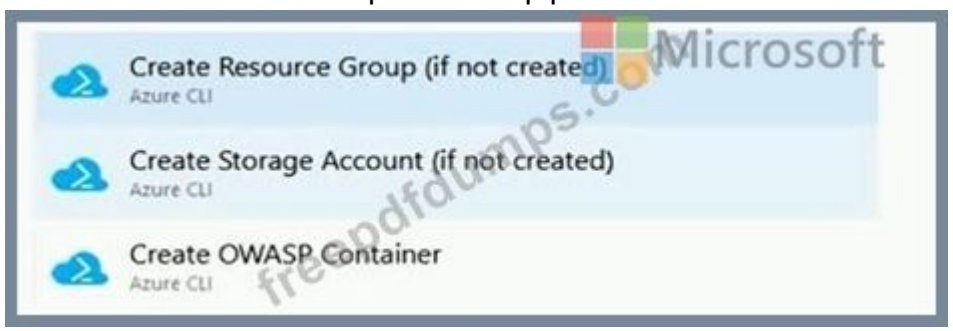
This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure DevOps project.

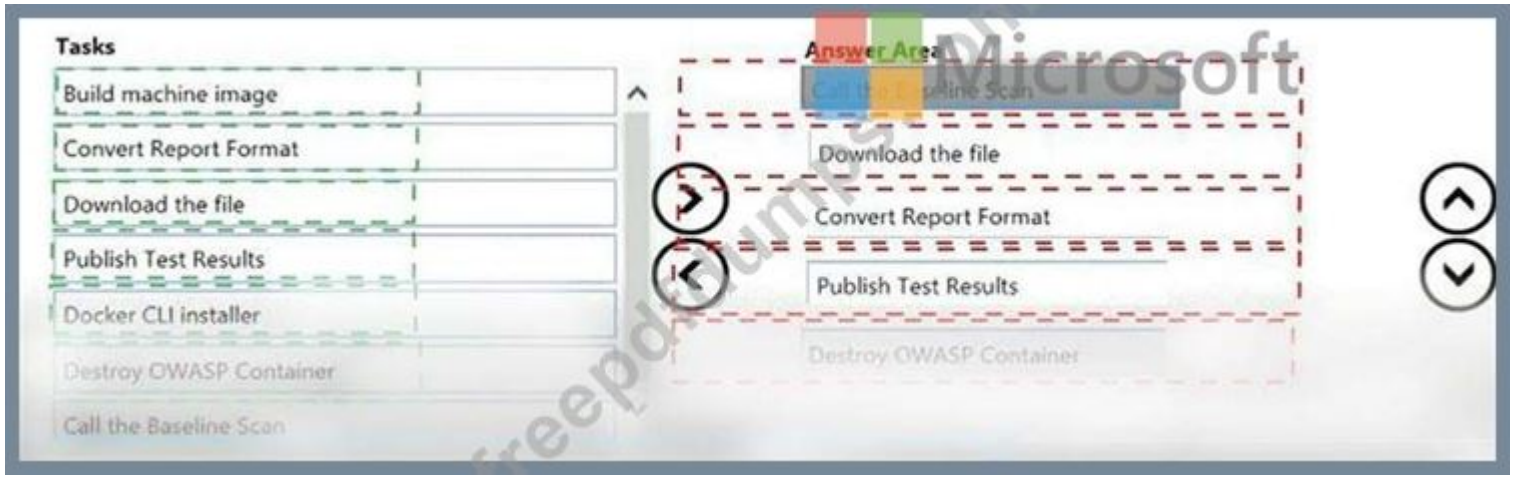
Your build process creates several artifacts.
You need to deploy the artifacts to on-premises servers.
Solution: You deploy an Azure self-hosted agent to an on-premises server. You add a Copy and Publish Build Artifacts task to the deployment pipeline.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
Explanation
To build your code or deploy your software using Azure Pipelines, you need at least one agent.
If your on-premises environments do not have connectivity to a Microsoft-hosted agent pool (which is typically the case due to intermediate firewalls), you'll need to manually configure a self-hosted agent on on-premises computer(s). The agents must have connectivity to the target on-premises environments, and access to the Internet to connect to Azure Pipelines or Team Foundation Server.
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops

NEW QUESTION: 251
You have an Azure DevOps release pipeline as shown in the following exhibit.

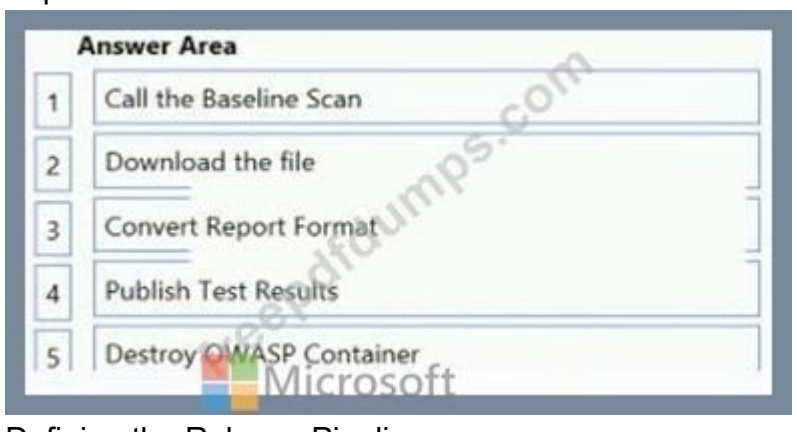


You need to complete the pipeline to configure OWASP ZAP for security testing.
Which five Azure CLI tasks should you add in sequence? To answer, move the tasks from the list of tasks to the answer area and arrange them in the correct order.

Answer:



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:

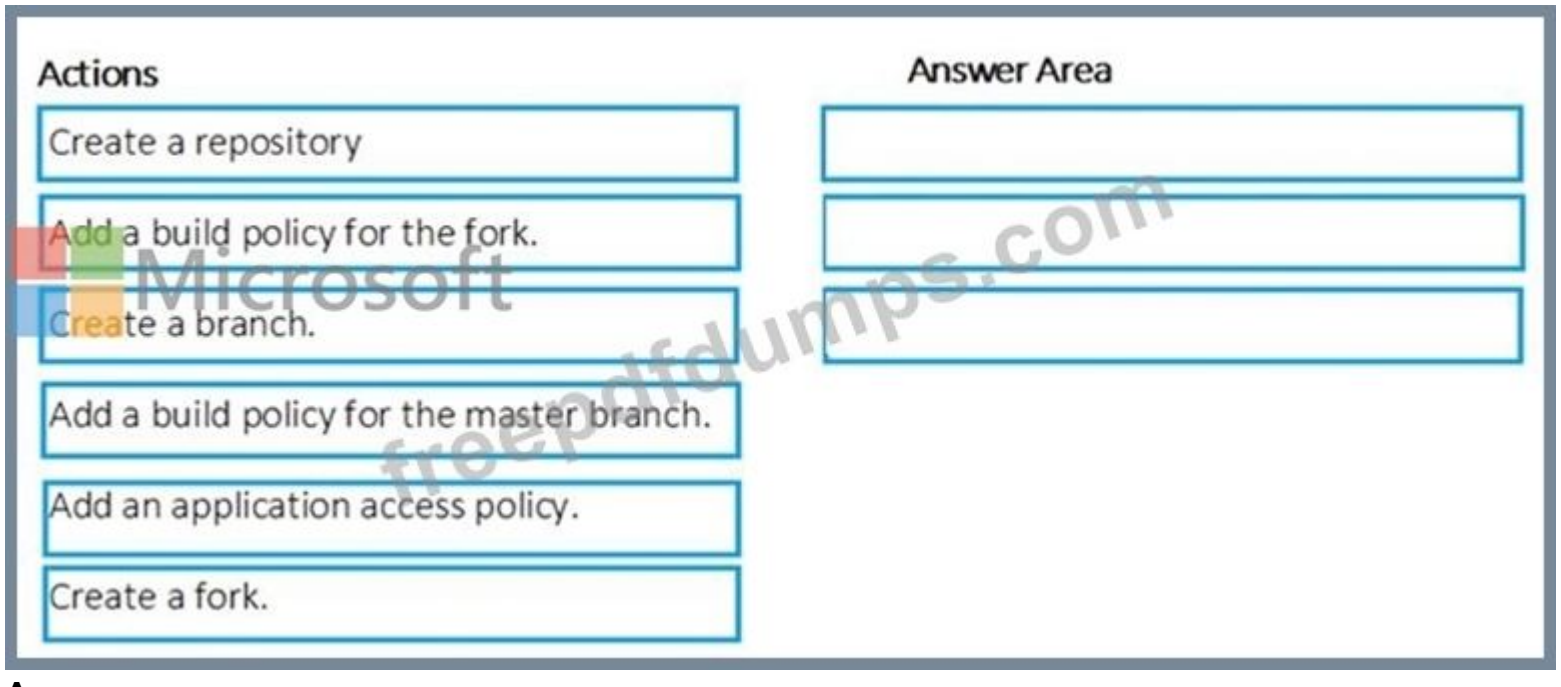
https://devblogs.microsoft.com/premier-developer/azure-devops-pipelines-leveraging-owasp-zap-in-the-release-p

NEW QUESTION: 252
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: (SHOW ANSWER)
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/

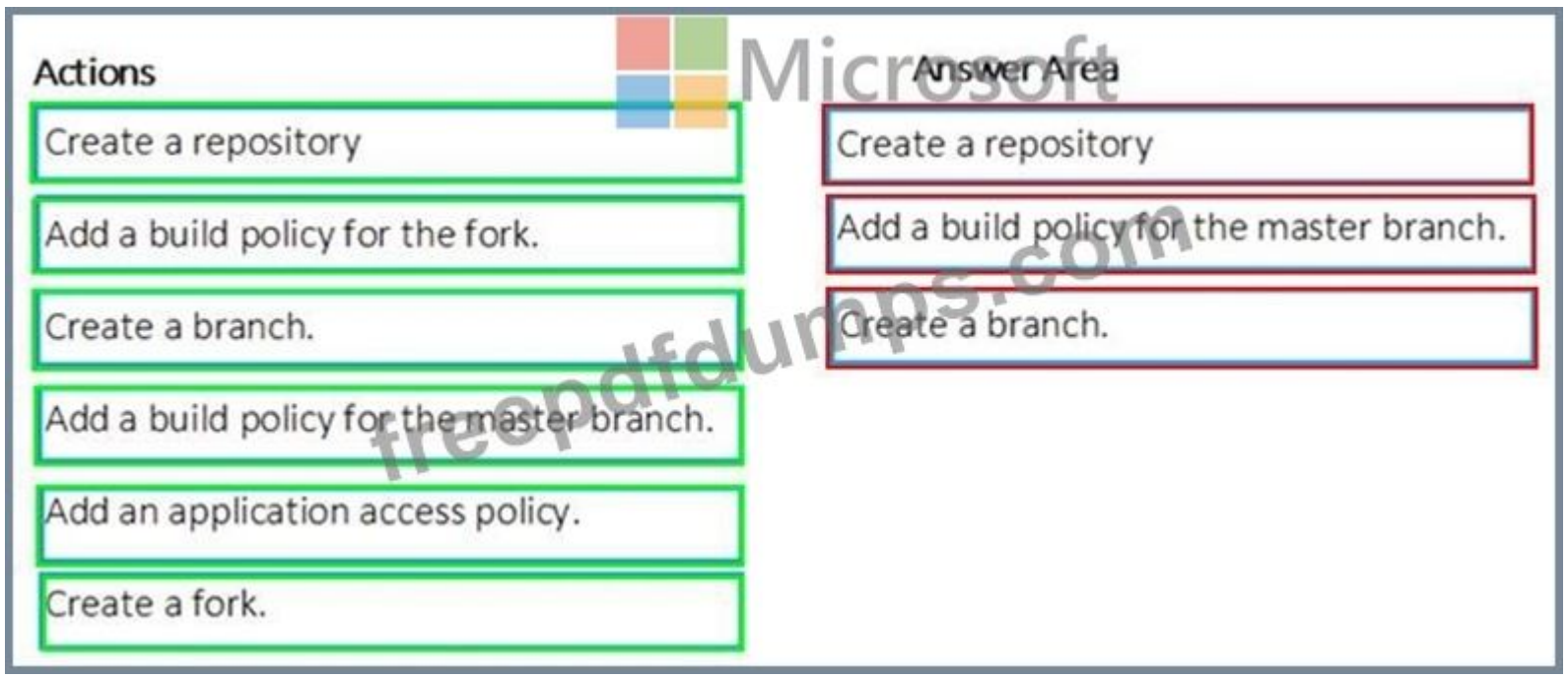
NEW QUESTION: 253
You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 that is configured for autoscaling.
You use Azure DevOps to build a web app named App1 and deploy App1 to VMSS1. App1 is used heavily 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: (SHOW ANSWER)
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
NEW QUESTION: 254

Note: This question is part of * series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sett might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an approval process that contains a condition. The condition requires that releases be approved by a team leader before they are deployed.
You have a poky stating that approvals must occur within eight hour.
You discover that deployments fail if the approvals take longer than two hours.
You need to ensure that the deployments only fail if the approvals take longer than eight hours.
Solution: From Post-deployment conditions, you modify the Time between re-evaluation of gates option.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Explanation
Use a gate From Pre-deployment conditions instead.
References: https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates

NEW QUESTION: 255
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.



Answer:



NEW QUESTION: 256

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. Modify the Security settings of the GitHub organization.

C. Create an Azure Active Directory B2C (Azure AD B2C) tenant.

D. Register GitHub in Azure AD.

Answer: (SHOW ANSWER)

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

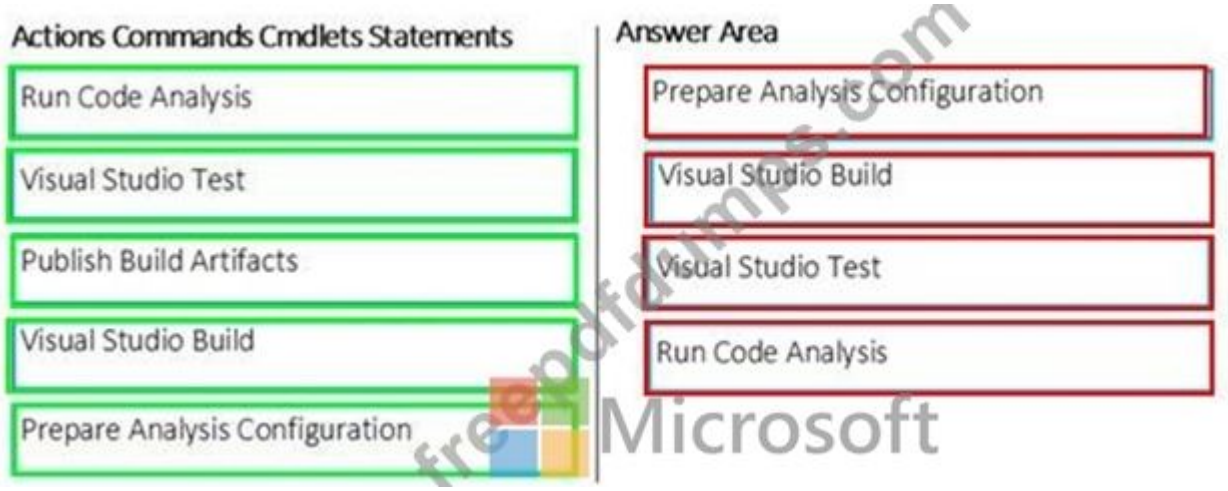
NEW QUESTION: 257

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You plan to create a release pipeline that will deploy Azure resources by using Azure Resource Manager templates. The release pipeline will create the following resources:
* Two resource groups
* Four Azure virtual machines in one resource group
* Two Azure SQL databases in other resource group
You need to recommend a solution to deploy the resources.
Solution: Create a main template that has two linked templates, each of which will deploy the resource in its respective group.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
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

NEW QUESTION: 258
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.

Answer:



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

NEW QUESTION: 259
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. Azure Active Directory Conditional Access Policy Validation
B. Alternate authentication credentials
C. Third-party application access via OAuth
D. SSH authentication

Answer: A (LEAVE A REPLY)
The Azure Pipelines app uses the OAuth authentication protocol, and requires Third-party application access via OAuth for the organization to be enabled. To enable this setting, navigate to Organization Settings > Security > Policies, and set the Third-party application access via OAuth for the organization setting to On.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams
Topic 1, Case Study Overview
Existing Environment
Litware, Inc. an independent software vendor (ISV) Litware has a main office and five branch offices.
Application Architecture
The company' s primary application is a single monolithic retirement fund management system based on ASP.NE T web forms that use logic written in V8.NET. Some new sections of the application are written in C#.
Variations of the application are created for individual customers. Currently, there are more than 80 have code branches in the application's code base.
The application was developed by using Microsoft Visual Studio. Source code is stored in Team Foundation Server (TFS) in the main office. The branch offices access of the source code by using TFS proxy servers.
Architectural Issues
Litware focuses on writing new code for customers. No resources are provided to refactor or remove existing code. Changes to the code base take a long time, AS dependencies are not obvious to individual developers.
Merge operations of the code often take months and involve many developers. Code merging frequently introduces bugs that are difficult to locate and resolve.
Customers report that ownership costs of the retirement fund management system increase continually. The need to merge unrelated code makes even minor code changes expensive.
Segmetn
Requirements
Planned Changes
Litware plans to develop a new suite of applications for investment planning. The investment planning Applications will require only minor integration with the easting retirement fund management system.
The investment planning applications suite will include one multi-tier web application and two iOS mobile applications. One mobile application will be used by employees; the other will be used by customers.
Litware plans to move to a more agile development methodology. Shared code will be extracted into a series of package.
Litware has started an internal cloud transformation process and plans to use cloud based services whenever suitable.
Litware wants to become proactive m detecting failures, rather than always waning for customer bug reports.
Technical Requirements
The company's investment planning applications suite must meet the following technical requirements:
* New incoming connections through the firewall must be minimized.
* Members of a group named Developers must be able to install packages.
* The principle of least privilege must be used for all permission assignments
* A branching strategy that supports developing new functionality in isolation must be used.
* Members of a group named Team leaders must be able to create new packages and edit the permissions of package feeds
* Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use.

* By default, all App Center must be used to centralize the reporting of mobile application crashes and device types in use.
* Code quality and release quality are critical. During release, deployments must not proceed between stages if any active bugs are logged against the release.
* The mobile applications must be able to call the share pricing service of the existing retirement fund management system. Until the system is upgraded, the service will only support basic authentication over HUPS.
* The required operating system configuration tor the test servers changes weekly. Azure Automation State Configuration must be used to ensure that the operating system on each test servers configured the same way when the servers are created and checked periodically.

Current Technical

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

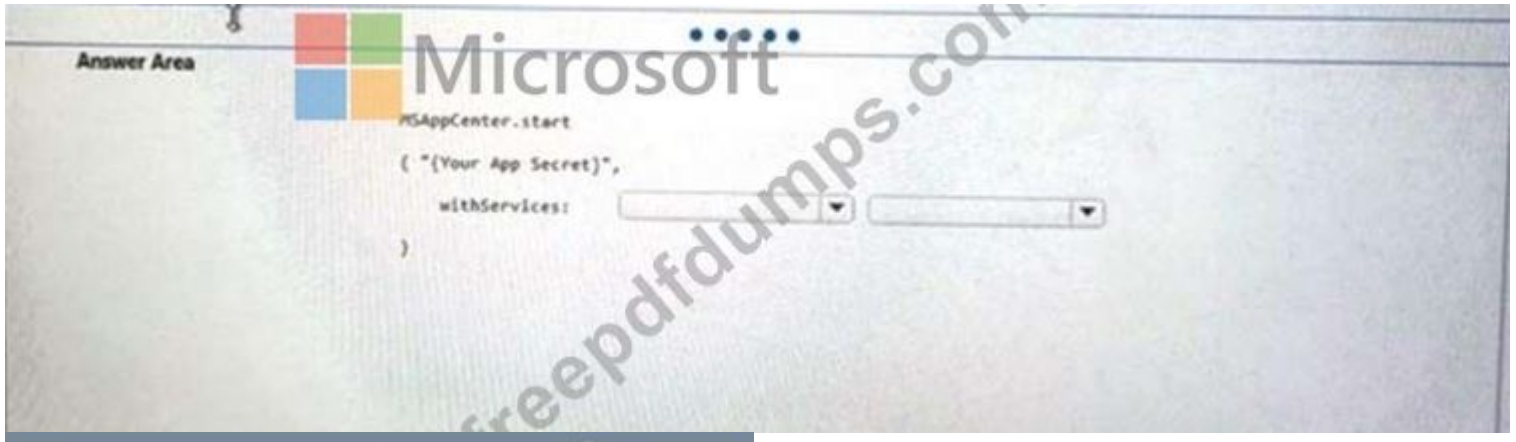
Azure Automation State Configuration nodes are registered by using the following command.

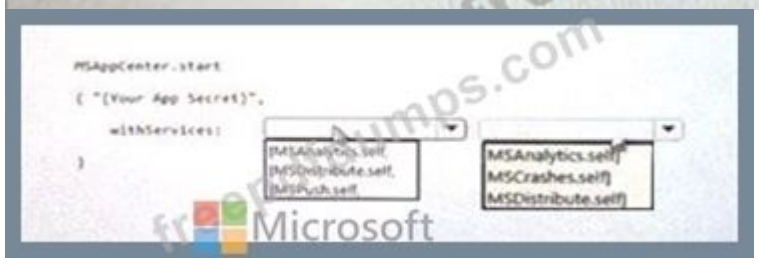
```
Register-AzureRmAutomationDscNode `
  -ResourceGroupName 'TestResourceGroup'
  -AutomationAccountName 'LitwareAutomationAccount'
  -AzureVMName $vmname
  -ConfigurationMode 'ApplyOnly'
```

NEW QUESTION: 260

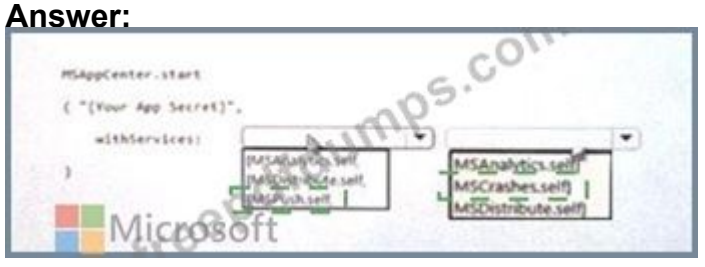
How should you complete the code to initialize App Center in the mobile application? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection a worth one point.





Answer:



NEW QUESTION: 261

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 (LEAVE A REPLY)

Explanation/Reference:

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

NEW QUESTION: 262

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:

Explanation:

Box 1: Azure Pipelines service connection

Box 2: Managed Service Identity Authentication

The managed identities for Azure resources feature in Azure Active Directory (Azure AD) provides Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code.

Reference:

https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/deploy/azure-key-vault

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

NEW QUESTION: 263

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?

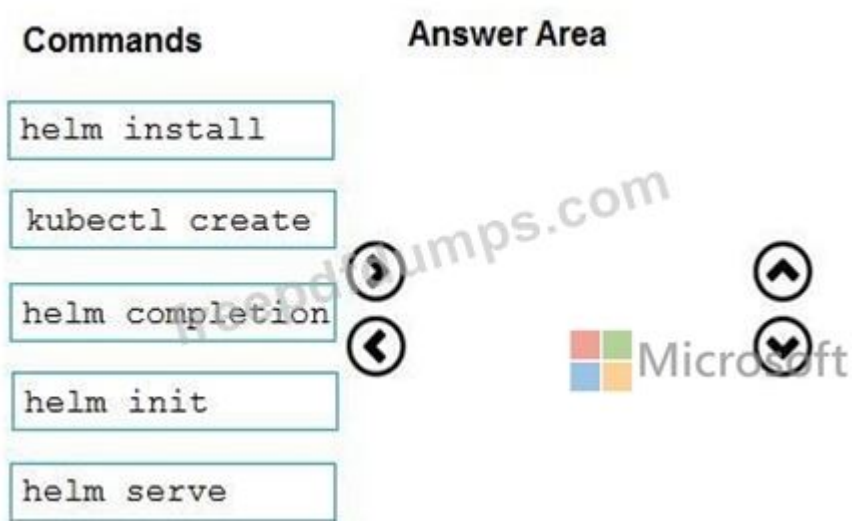
A. Cobertura
B. Bullseye Coverage
C. MSTest
D. Coverlet
E. NUnit
F. Coverage.py
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Use Publish Code Coverage Results task in a build pipeline to publish code coverage results to Azure Pipelines or TFS, which were produced by a build in Cobertura or JaCoCo format.
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-code-coverage-results

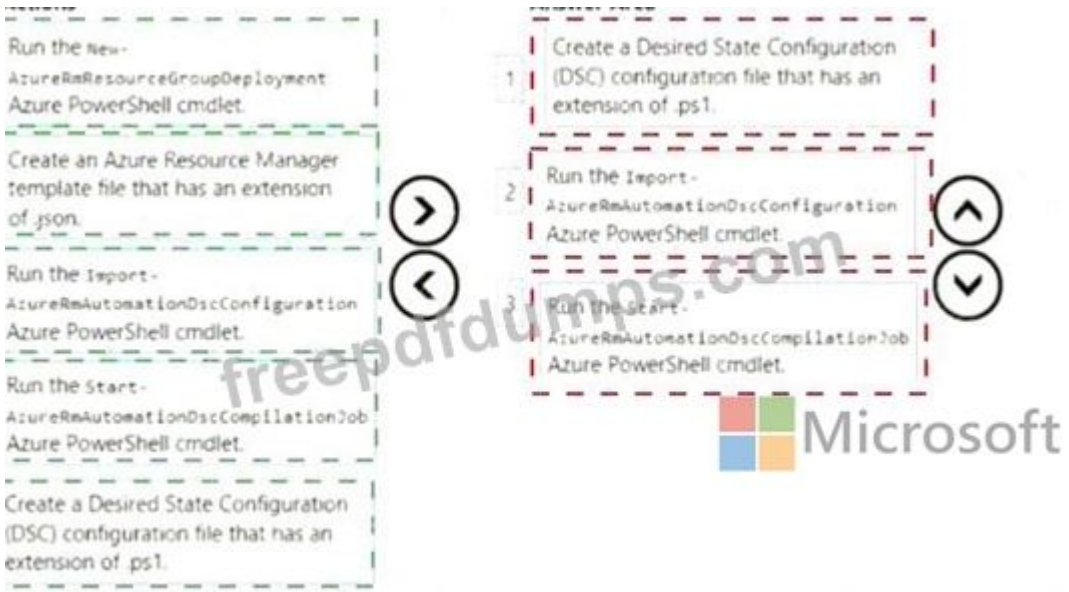
NEW QUESTION: 264
What should you use to implement the code quality restriction on the release pipeline for the investment planning applications suite?
A. a pre-deployment approval
B. a deployment gate
C. a post-deployment approval
D. a trigger
Answer: (SHOW ANSWER)
When a release is created from a release 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 Implement Continuous Delivery Question Set 2

NEW QUESTION: 265
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:
You can authenticate as a GitHub App.
References: https://developer.github.com/apps/building-github-apps/authenticating-with-github-apps/

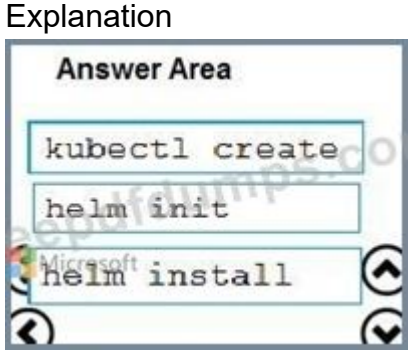
NEW QUESTION: 266
You have a Microsoft ASP.NET Core web app in Azure that is accessed worldwide.
You need to run a URL ping test once every five minutes and create an alert when the web app is unavailable from specific Azure regions. The solution must minimize development time.
What should you do?
A. 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 (LEAVE A REPLY)
There are three types of Application Insights availability tests:
* URL ping test: a simple test that you can create in the Azure portal.
* Multi-step web test
* Custom Track Availability Tests
Note: After you've deployed your web app/website, you can set up recurring tests to monitor availability and responsiveness. Azure Application Insights sends web requests to your application at regular intervals from points around the world. It can alert you if your application isn't responding, or if it responds too slowly.
You can set up availability tests for any HTTP or HTTPS endpoint that is accessible from the public internet.
You don't have to make any changes to the website you're testing. In fact, it doesn't even have to be a site you own. You can test the availability of a REST API that your service depends on.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability#create-a-url-ping-test

NEW QUESTION: 267
You need to recommend a solution for deploying charts by using Helm and Title to Azure Kubemets Service (AKS) in an RBAC-enabled cluster.
Which three commands should you recommend be run m sequence? To answer, move the appropriate commands from the list of commands to the answer area and arrange them in the correct order.





Explanation



Step 1: Kubectl create

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

Example: Service account with cluster-admin role

$ kubectl create -f rbac-config.yaml

serviceaccount "tiller" created

clusterrolebinding "tiller" created

$ helm init --service-account tiller

Step 2: helm init

To deploy a basic Tiller into an AKS cluster, use the helm init command.

Step 3: helm install

To install charts with Helm, use the helm install command and specify the name of the chart to install.

References:

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

https://docs.helm.sh/using_helm/#tiller-namespaces-and-rbac

NEW QUESTION: 268

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 action should you include in the recommendation?

A. Configure post-deployment approvals in the deployment pipeline.

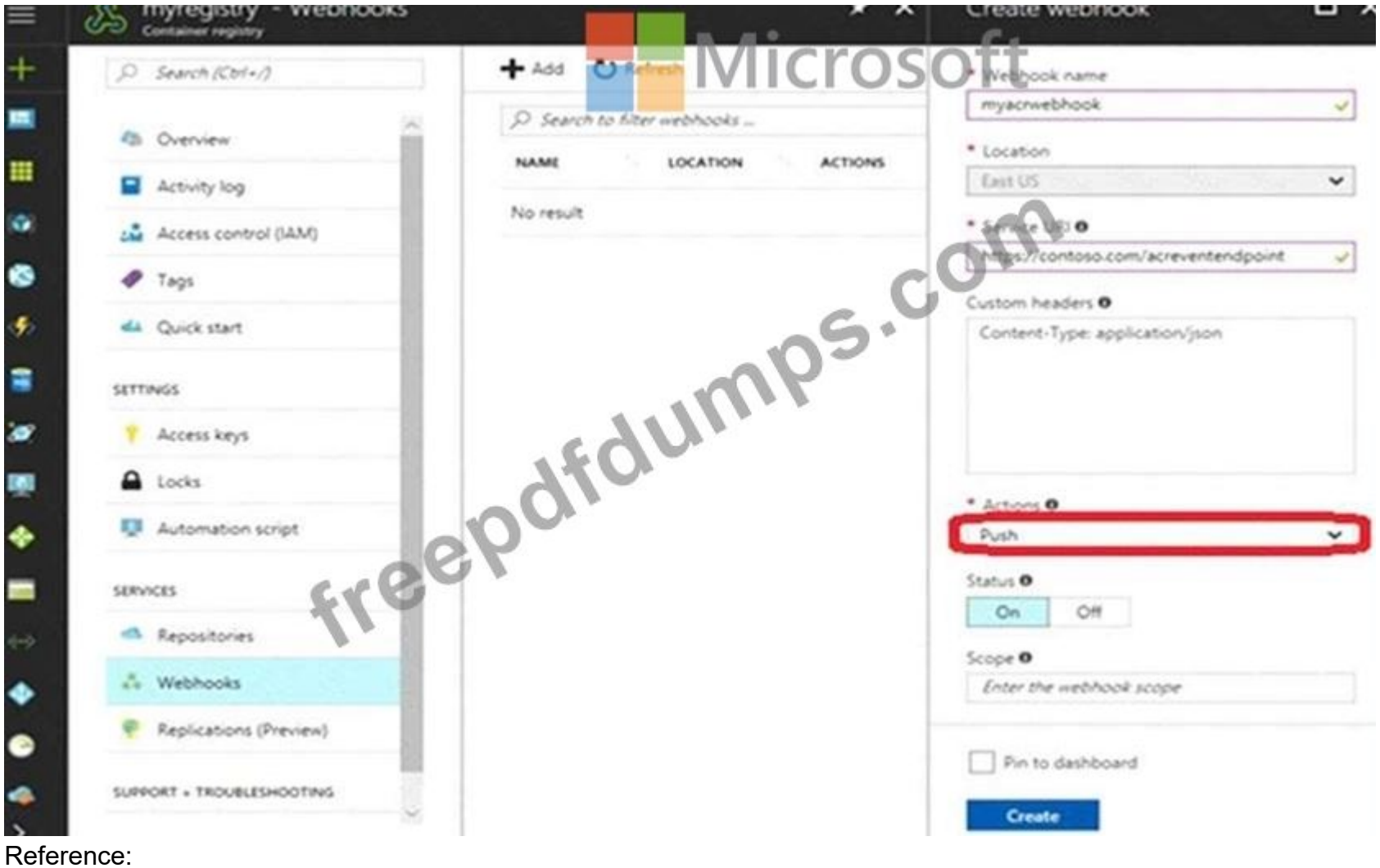
B. Integrate Azure DevOps and SonarQube.
C. Integrate Azure DevOps and Azure DevTest Labs.
Answer: (SHOW ANSWER)
Explanation
You can manage technical debt with SonarQube and Azure DevOps.
Note: Technical debt is the set of problems in a development effort that make forward progress on customer value inefficient. Technical debt saps productivity by making code hard to understand, fragile, time-consuming to change, difficult to validate, and creates unplanned work that blocks progress. Unless they are managed, technical debt can accumulate and hurt the overall quality of the software and the productivity of the development team in the long term SonarQube an open source platform for continuous inspection of code quality to perform automatic reviews with static analysis of code to:
* Detect Bugs
* Code Smells
* Security Vulnerabilities
* Centralize Quality
* What's covered in this lab
Reference:
https://azuredevopslabs.com/labs/vstsextend/sonarqube/

NEW QUESTION: 269
Your company hosts a web application in Azure. The company uses Azure Pipelines for the build and release management of the application. Stakeholders report that the past few releases have negatively affected system performance.
You configure alerts in Azure Monitor.
You need to ensure that new releases are only deployed to production if the releases meet defined performance baseline criteria in the staging environment first.
What should you use to prevent the deployment of releases that fall to meet the performance baseline?
A. an Azure Scheduler job
B. a trigger
C. a gate
D. an Azure function
Answer: C (LEAVE A REPLY)
Scenarios and use cases for gates include:
Quality validation. Query metrics from tests on the build artifacts such as pass rate or code coverage and deploy only if they are within required thresholds.
Use Quality Gates to integrate monitoring into your pre-deployment or post-deployment. This ensures that you are meeting the key health/performance metrics (KPIs) as your applications move from dev to production and any differences in the infrastructure environment or scale is not negatively impacting your KPIs.
Note: Gates allow automatic collection of health signals from external services, and then promote the release when all the signals are successful at the same time or stop the deployment on timeout. Typically, gates are used in connection with incident management, problem management, change management, monitoring, and external approval systems.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/continuous-monitoring

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

NEW QUESTION: 270
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 (LEAVE A REPLY)
Separate Your Dependencies
Within your package.json file be sure you split out your npm dependencies between devDependencies and (production) dependencies. The key part is that you must then make use of the --production flag when installing the npm packages. The --production flag will exclude all packages defined in the devDependencies section.
References: https://blogs.msdn.microsoft.com/visualstudioalmrangers/2017/06/08/manage-your-open-source- usage-and-security-as-reported-by-your-cicd-pipeline/

NEW QUESTION: 271
You need to ensure that the https://contoso.com/statushook webhook is called every time a repository named az40010480345acr1 receives a new version of an image named dotnetapp.
To complete this task, sign in to the Microsoft Azure portal.
Answer:
See solution below.
Explanation
* Sign in to the Azure portal.
* Navigate to the container registry az40010480345acr1.
* Under Services, select Webhooks.
* Select the existing webhook https://contoso.com/statushook, and double-click on it to get its properties.
* For Trigger actions select image push
Example web hook:



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

NEW QUESTION: 272
Your company is building a new web application.
You plan to collect feedback from pilot users on the features being delivered.
All the pilot users have a corporate computer that has Google Chrome and the Microsoft Test & Feedback extension installed. The pilot users will test the application by using Chrome.
You need to identify which access levels are required to ensure that developers can request and gather feedback from the pilot users. The solution must use the principle of least privilege.
Which access levels m Azure DevOps should you identify? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Box 1: Basic

Assign Basic to users with a TFS CAL, with a Visual Studio Professional subscription, and to users for whom you are paying for Azure Boards & Repos in an organization.

Box 2: Stakeholder

Assign Stakeholders to users with no license or subscriptions who need access to a limited set of features.

Note:

You assign users or groups of users to one of the following access levels:

Basic: provides access to most features

VS Enterprise: provides access to premium features

Stakeholders: provides partial access, can be assigned to unlimited users for free References: https://docs.microsoft.com/en-us/azure/devops/organizations/security/access-levels?view=vsts

NEW QUESTION: 273

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

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

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

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

Solution: You add a trigger to the build pipeline.

Does this meet the goal?

A. Yes

B. No

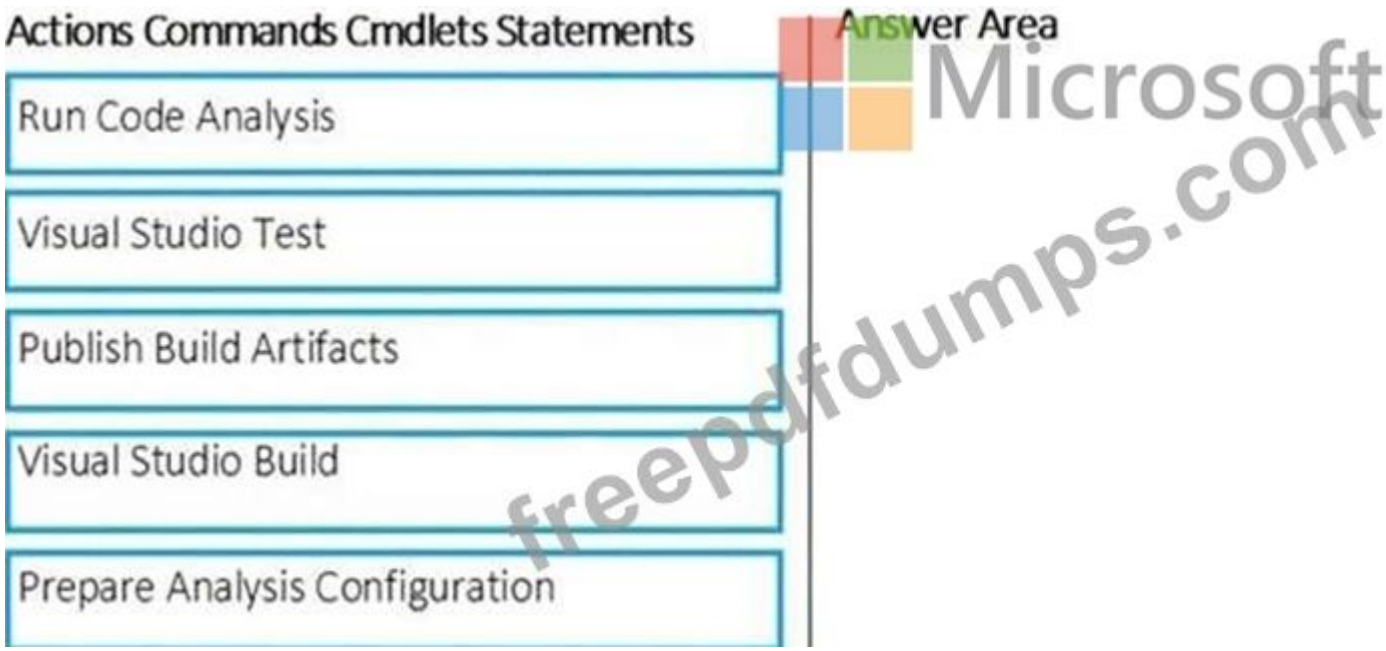
Answer: B (LEAVE A REPLY)

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

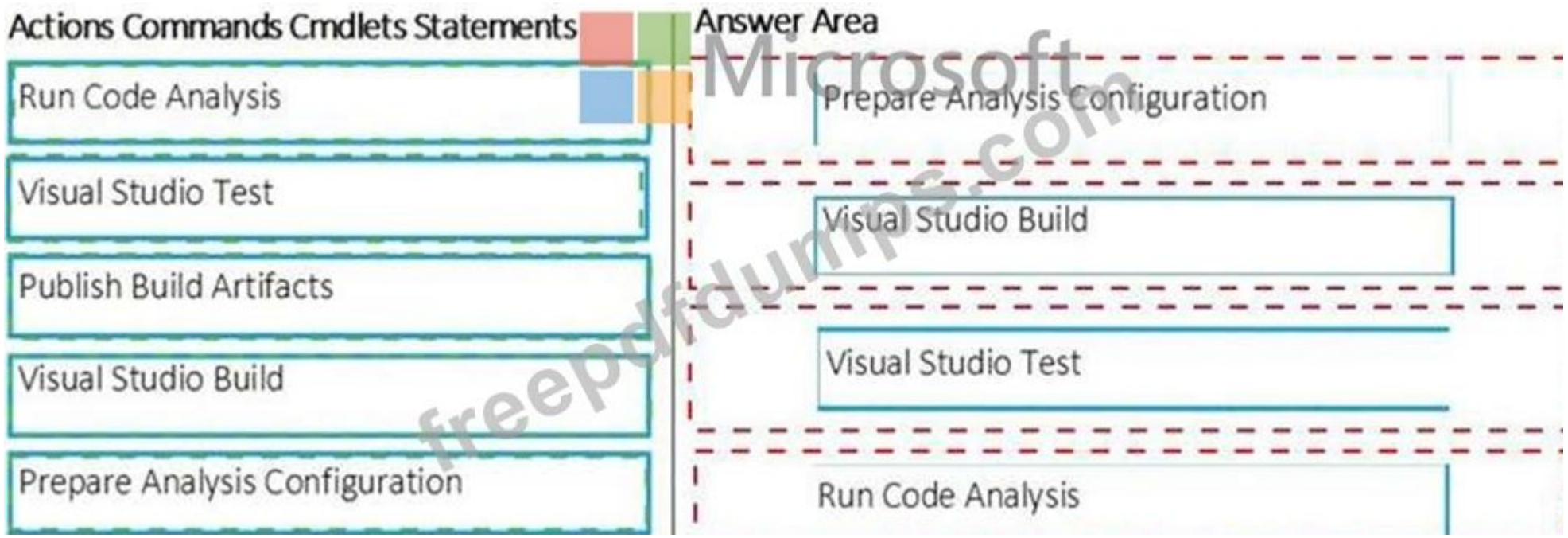
References:

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

NEW QUESTION: 274
DRAG DROP
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.



Answer:



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

NEW QUESTION: 275
Your company uses Service Now for incident management.
You develop an application that runs on Azure.
The company needs to generate a ticket in Service Now when the application fails to authenticate.
Which Azure Log Analytics solution should you use?
A. Automation & Control
B. IT Service Management Connector (ITSM)
C. Application lmiQ.hu Connector
D. insight & Analytics
Answer: (SHOW ANSWER)
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

NEW QUESTION: 276
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 (LEAVE A REPLY)
ACR Tasks supports automated container image builds when a container's base image is updated, such as when you patch the OS or application framework in one of your base images.
Reference:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-tutorial-base-image-update

NEW QUESTION: 277

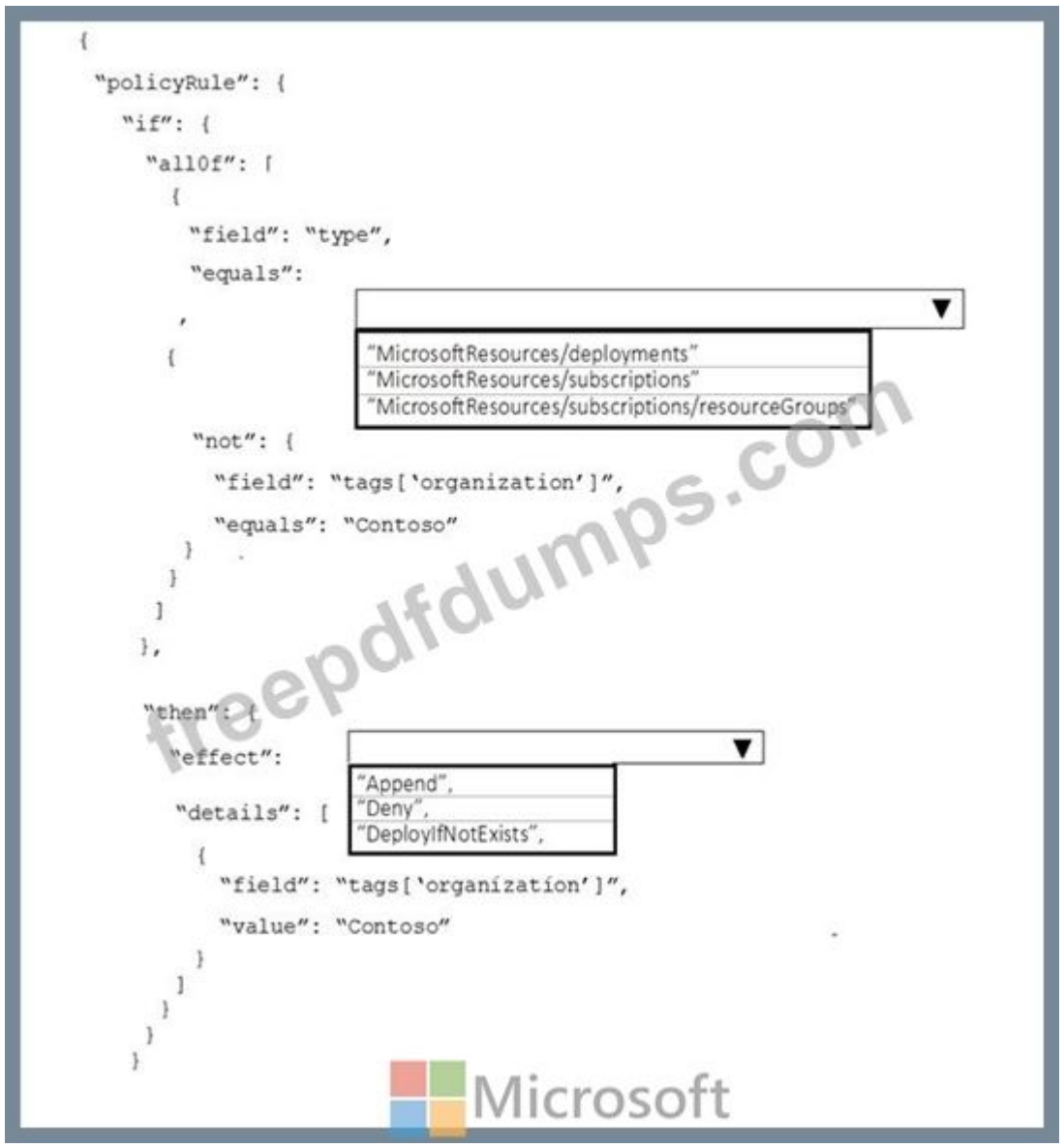
Your company has an Azure subscription.

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:

Explanation:

Box 1: " Microsoft.Resources/subscriptions/resourceGroups"

Box 2: "Deny",

Sample - Enforce tag and its value on resource groups

},

"policyRule": {

"if": {

"allOf": [

{

"field": "type",

"equals": "Microsoft.Resources/subscriptions/resourceGroups"

},

{

"not": {

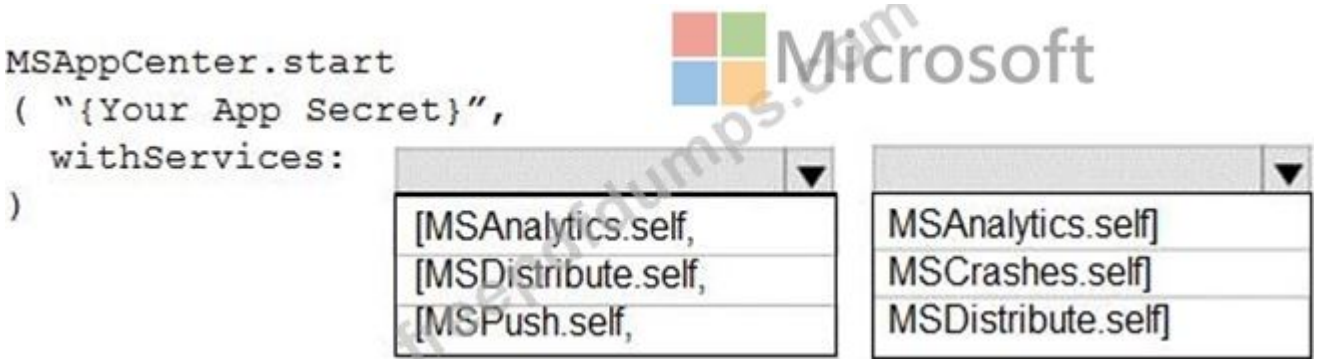
"field": "[concat('tags[',parameters('tagName'), ']')]",

"equals": "[parameters('tagValue')]"

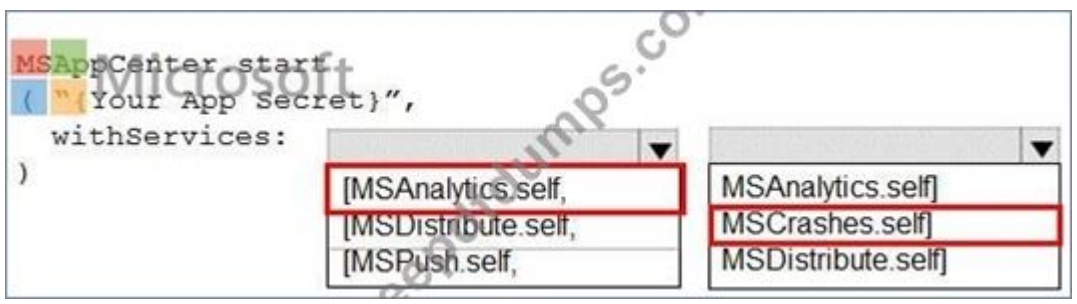
}

}
]
},
"then": {
"effect": "deny"
}
}
}
}
References:
https://docs.microsoft.com/en-us/azure/governance/policy/samples/enforce-tag-on-resource-groups

NEW QUESTION: 278
How should you complete the code to initialize App Center in the mobile application? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection a worth one point.



Answer:

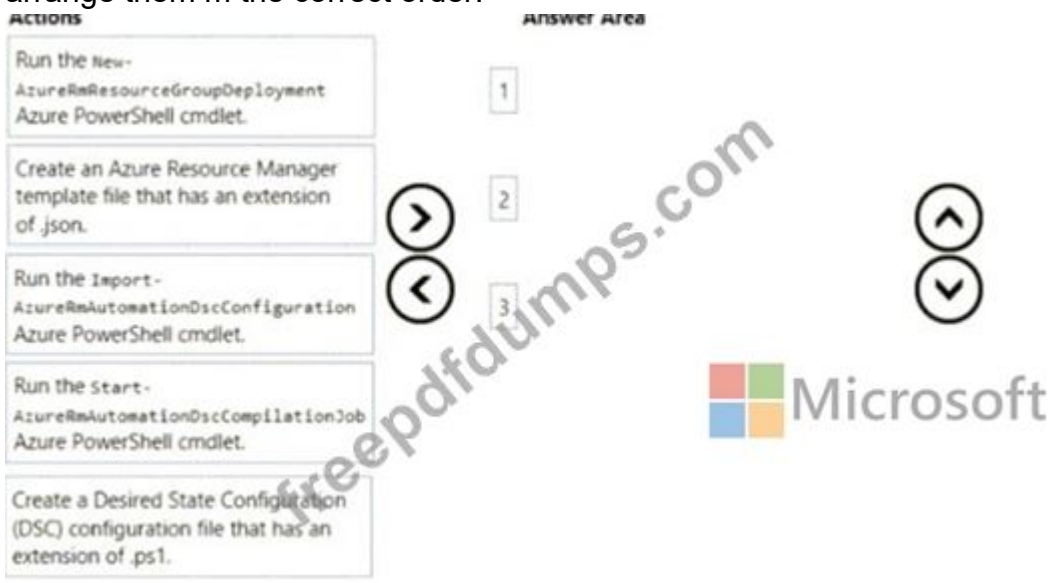


Explanation:
Scenario: Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use.
In order to use App Center, you need to opt in to the service(s) that you want to use, meaning by default no services are started and you will have to explicitly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

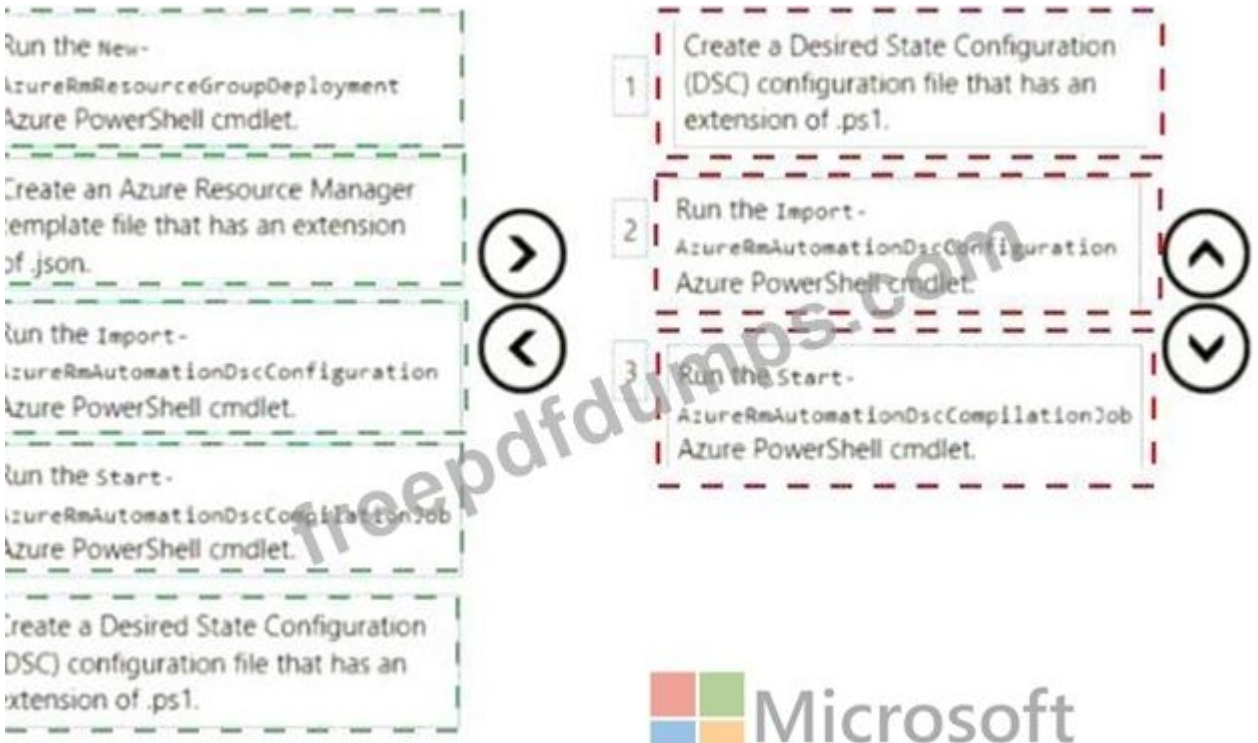
NEW QUESTION: 279
Your company is building a new solution in Java.
The company currently uses a SonarQube server to analyze the code of .NET solutions.

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 (LEAVE A REPLY)
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/

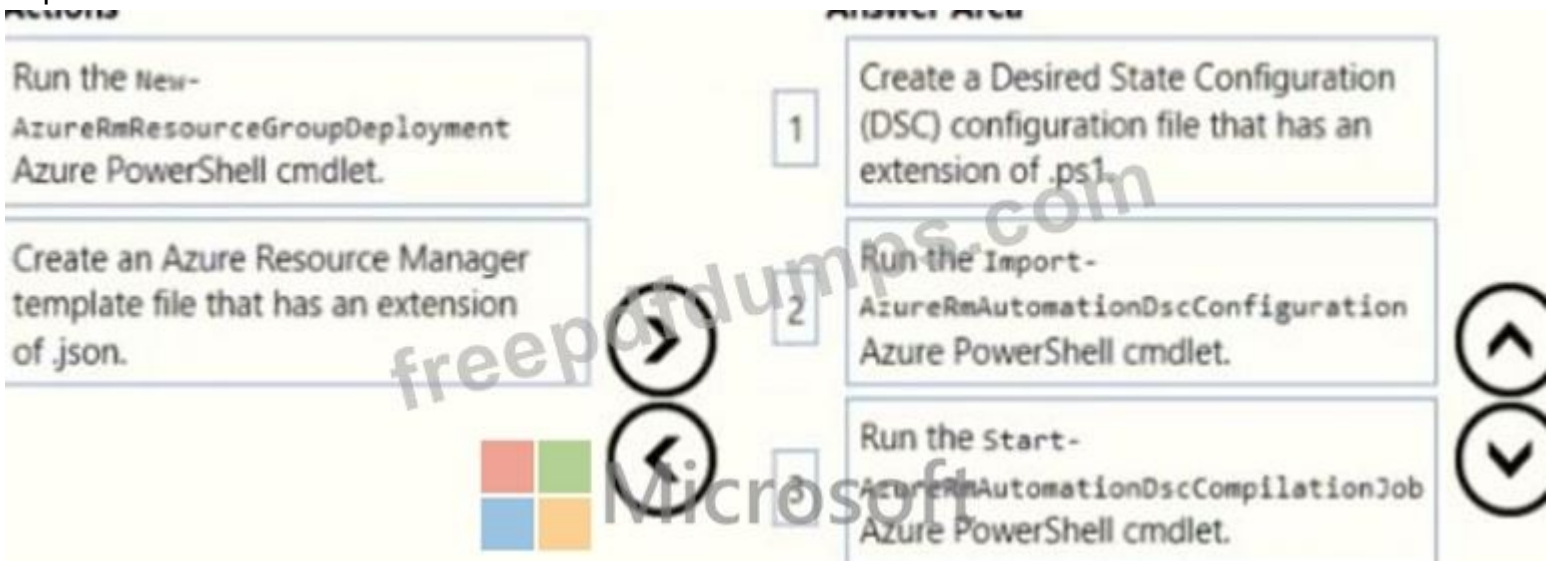
NEW QUESTION: 280
You need to configure Azure Automation for the computers in Pool7.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them m the correct order.



Answer:



Explanation



NEW QUESTION: 281
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: B,D (LEAVE A REPLY)

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

NEW QUESTION: 282
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.
You need to recommend changes to reduce the accumulated technical debt.
Solution: You recommend increasing the test coverage.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Explanation
Instead reduce the code complexity.
Reference:
https://dzone.com/articles/fight-through-the-pain-how-to-deal-with-technical

NEW QUESTION: 283
Your company has a hybrid cloud between Azure and Azure Stack.
The company uses Azure DevOps for its CI/CD pipelines. Some applications are built by using Erlang and Hack.
You need to ensure that Erlang and Hack are supported as part of the build strategy across the hybrid cloud.
The solution must minimize management overhead.
What should you use to execute the build pipeline?
A. AzureDevOps self-hosted agents on Azure DevTest Labs virtual machines.
B. AzureDevOps self-hosted agents on virtual machine that run on Azure Stack
C. AzureDevOps self-hosted agents on Hyper-V virtual machines
D. a Microsoft-hosted agent

Answer: (SHOW ANSWER)

Explanation

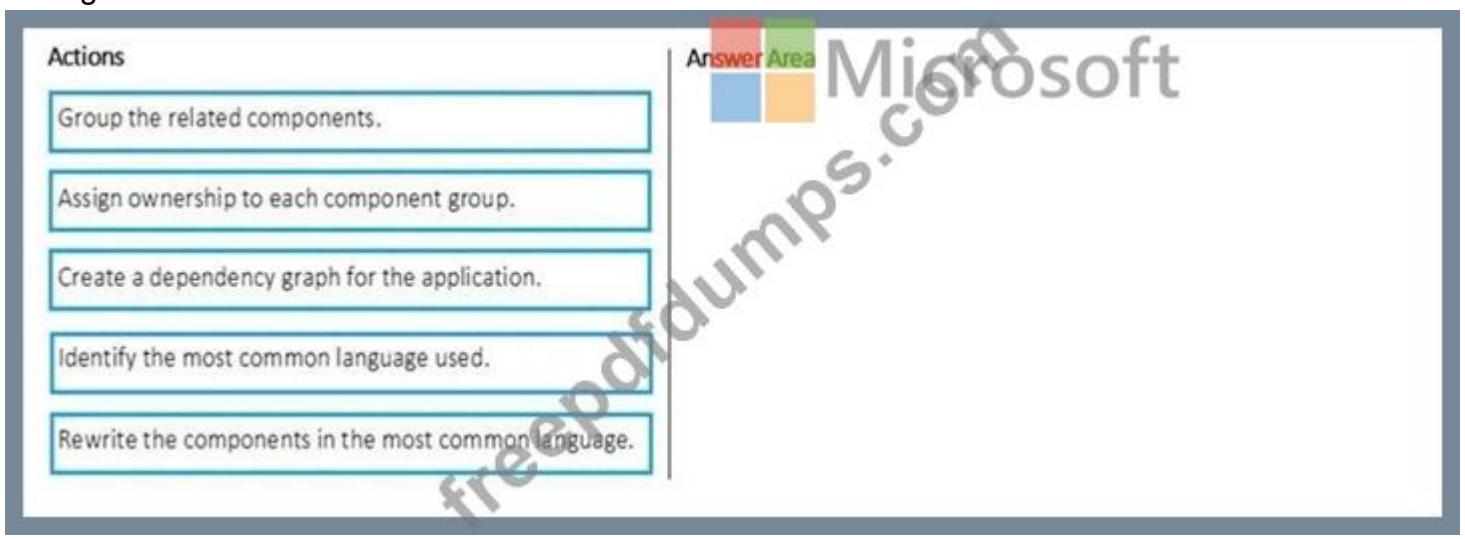
Azure Stack offers virtual machines (VMs) as one type of an on-demand, scalable computing resource. You can choose a VM when you need more control over the computing environment.

References: https://docs.microsoft.com/en-us/azure/azure-stack/user/azure-stack-compute-overview

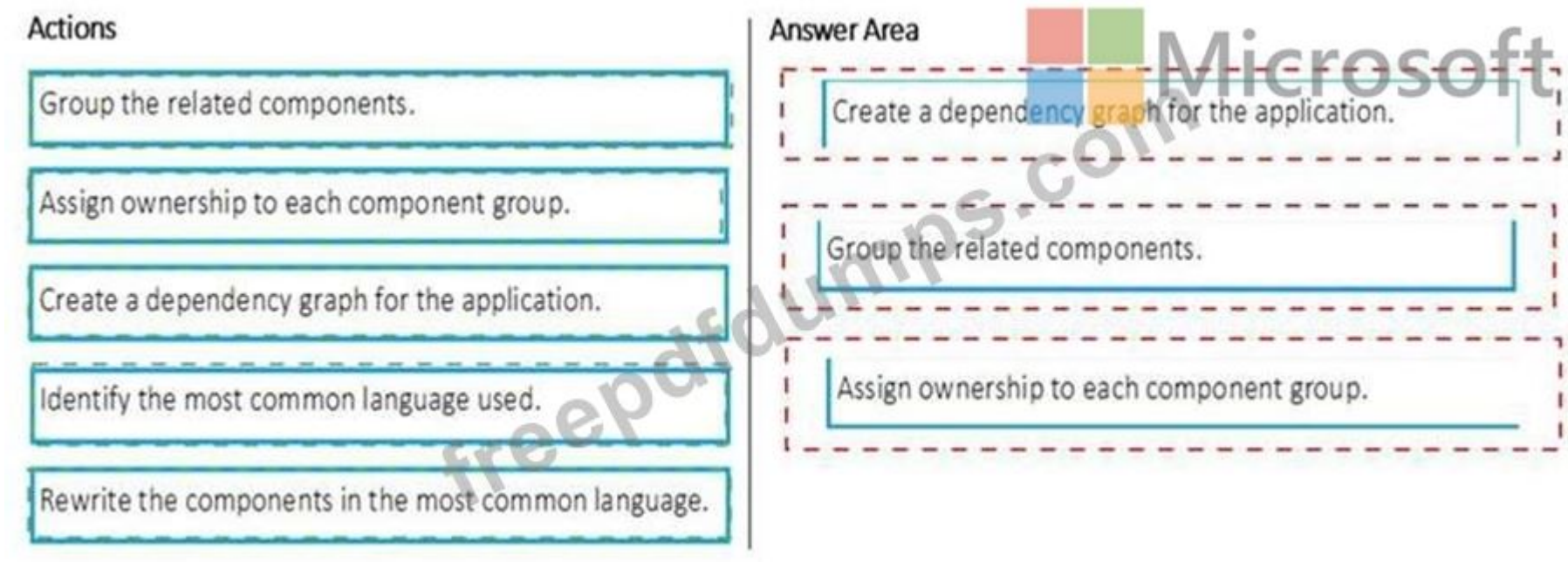
NEW QUESTION: 284

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

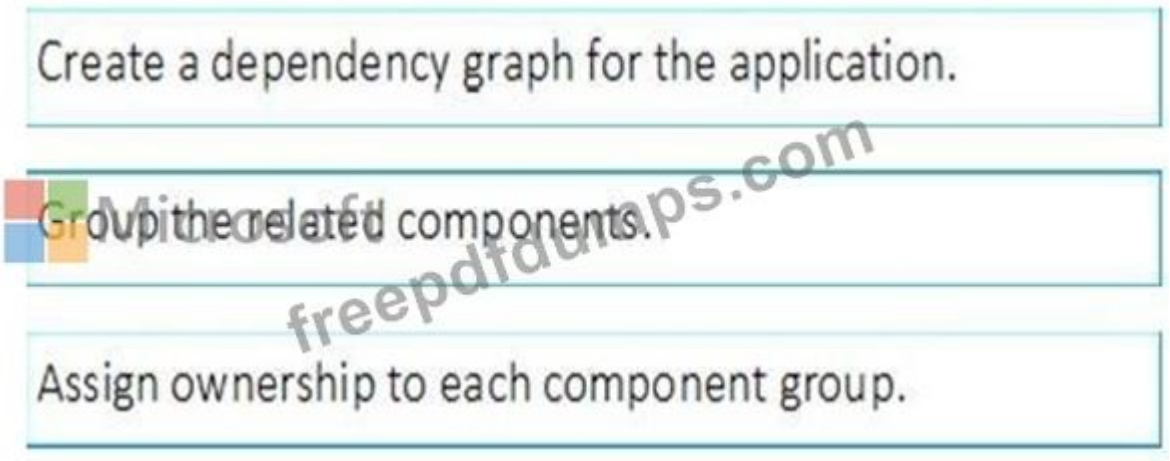
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation



Step 1: Create a dependency graph for the application

By linking work items and other objects, you can track related work, dependencies, and changes made over time. All links are defined with a specific link type. For example, you can use Parent/Child links to link work items to support a hierarchical tree structure. Whereas, the Commit and Branch link types support links between work items and commits and branches, respectively.

Step 2: Group the related components.

Packages enable you to share code across your organization: you can compose a large product, develop multiple products based on a common shared framework, or create and share reusable components and libraries.

Step 3: Assign ownership to each component graph

References:

https://docs.microsoft.com/en-us/azure/devops/boards/queries/link-work-items-support-traceability?view=azure-

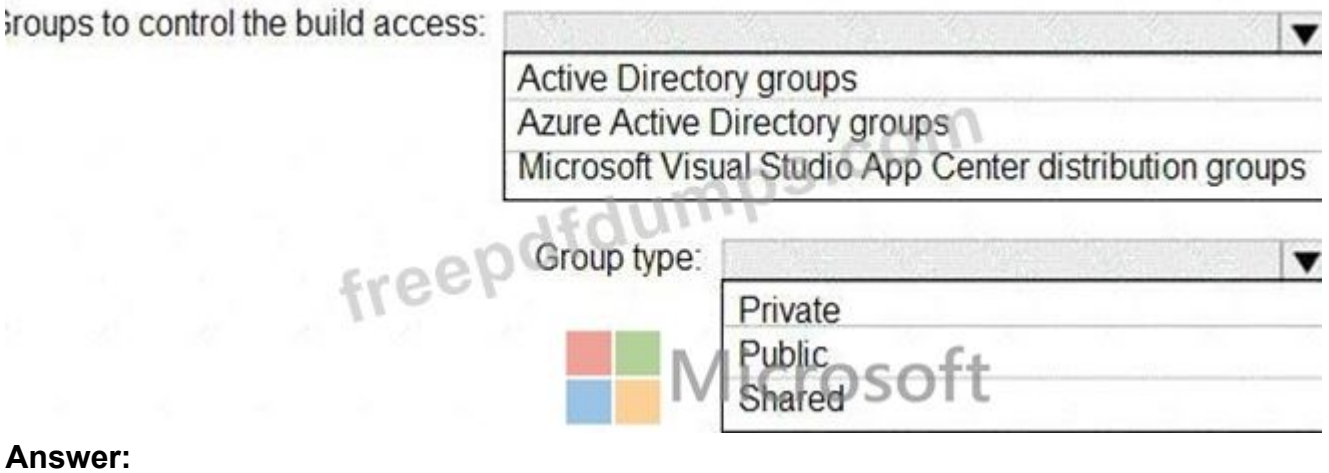
https://docs.microsoft.com/en-us/visualstudio/releasenotes/tfs2017-relnotes

NEW QUESTION: 285

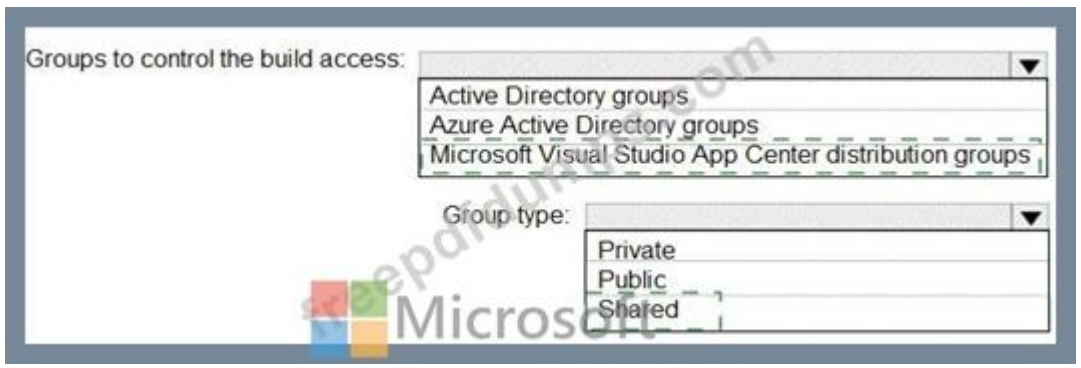
Your company is creating a suite of three mobile applications.

You need to control access to the application builds. The solution must be managed at the organization level What should you use? To answer, select the appropriate options m the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation

Box 1: Microsoft Visual Studio App Center distribution Groups

Distribution Groups are used to control access to releases. A Distribution Group represents a set of users that can be managed jointly and can have common access to releases. Example of Distribution Groups can be teams of users, like the QA Team or External Beta Testers or can represent stages or rings of releases, such as Staging.

Box 2: Shared

Shared distribution groups are private or public distribution groups that are shared across multiple apps in a single organization. Shared distribution groups eliminate the need to replicate distribution groups across multiple apps.

Note: With the Deploy with App Center Task in Visual Studio Team Services, you can deploy your apps from Azure DevOps (formerly known as VSTS) to App Center. By deploying to App Center, you will be able to distribute your builds to your users.

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

NEW QUESTION: 286

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 (LEAVE A REPLY)

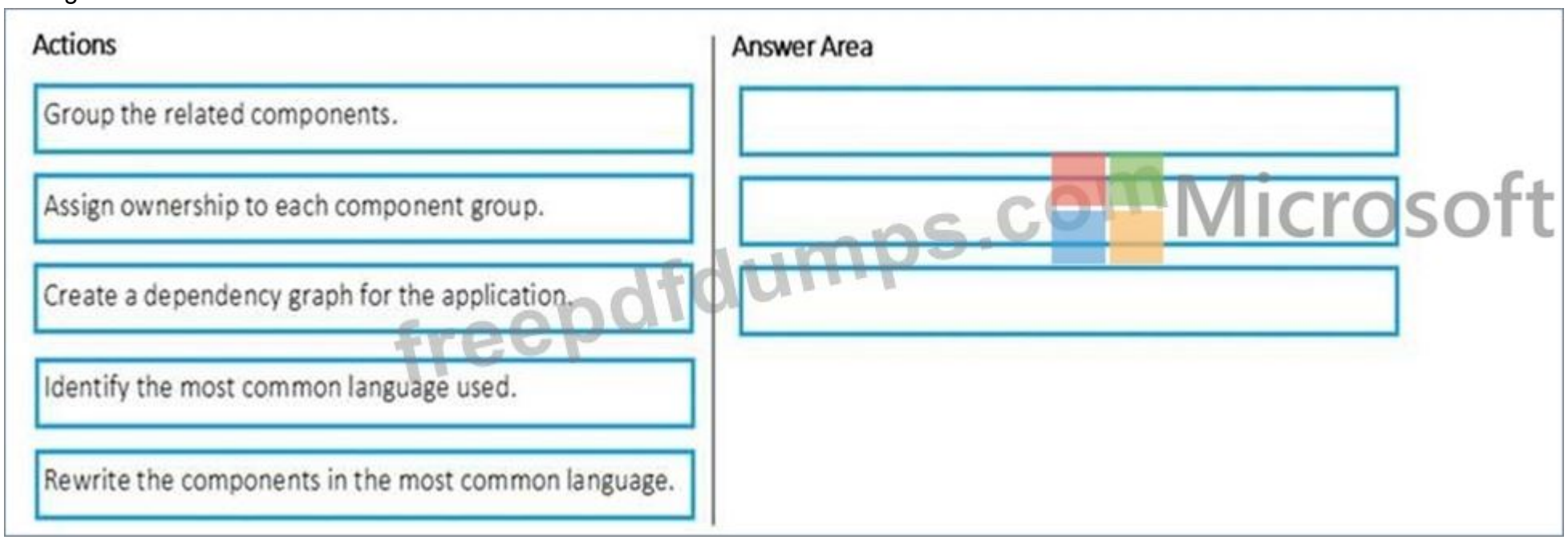
Explanation

WhiteSource is the leader in continuous open source software security and compliance management.

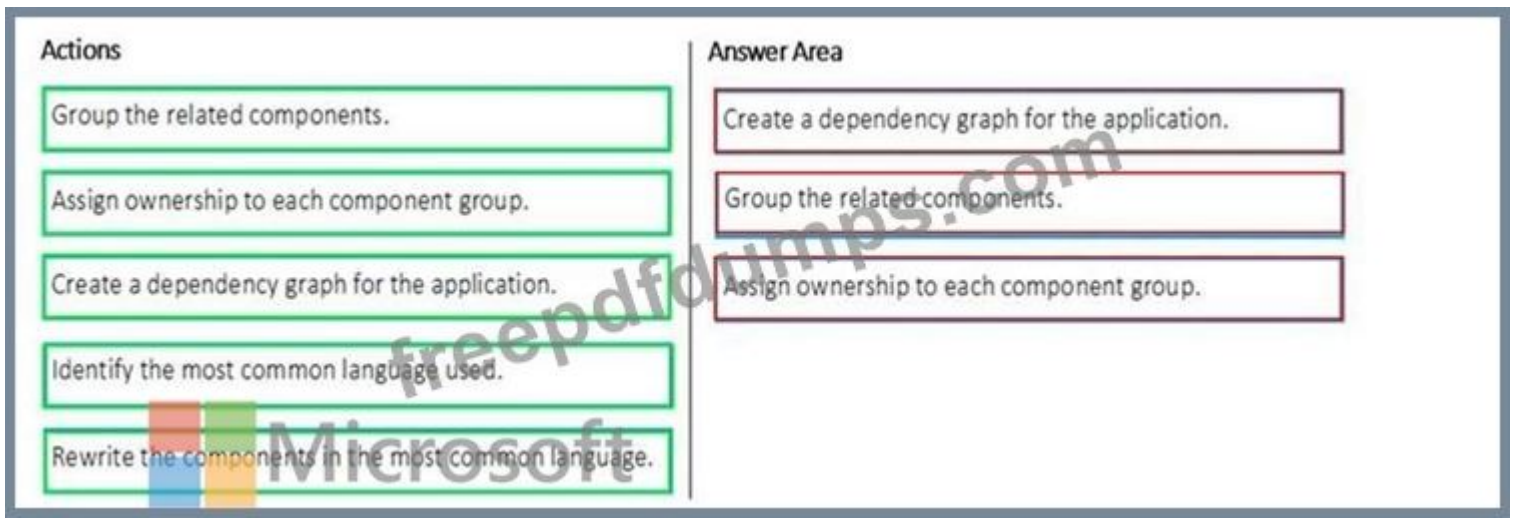
WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against

WhiteSource constantly-updated denitive database of open source repositories.
Azure DevOps integration with WhiteSource Bolt will enable you to:
* Detect and remedy vulnerable open source components.
* Generate comprehensive open source inventory reports per project or build.
* Enforce open source license compliance, including dependencies' licenses.
* Identify outdated open source libraries with recommendations to update.
References: https://www.azuredevopslabs.com/labs/vstsextend/WhiteSource/

NEW QUESTION: 287
You need to find and isolate shared code. The shared code will be maintained in a series of packages.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:

Step 1: Create a dependency graph for the application

By linking work items and other objects, you can track related work, dependencies, and changes made over time. All links are defined with a specific link type. For example, you can use Parent/Child links to link work items to support a hierarchical tree structure. Whereas, the Commit and Branch link types support links between work items and commits and branches, respectively.

Step 2: Group the related components.

Packages enable you to share code across your organization: you can compose a large product, develop multiple products based on a common shared framework, or create and share reusable components and libraries.

Step 3: Assign ownership to each component graph

References:

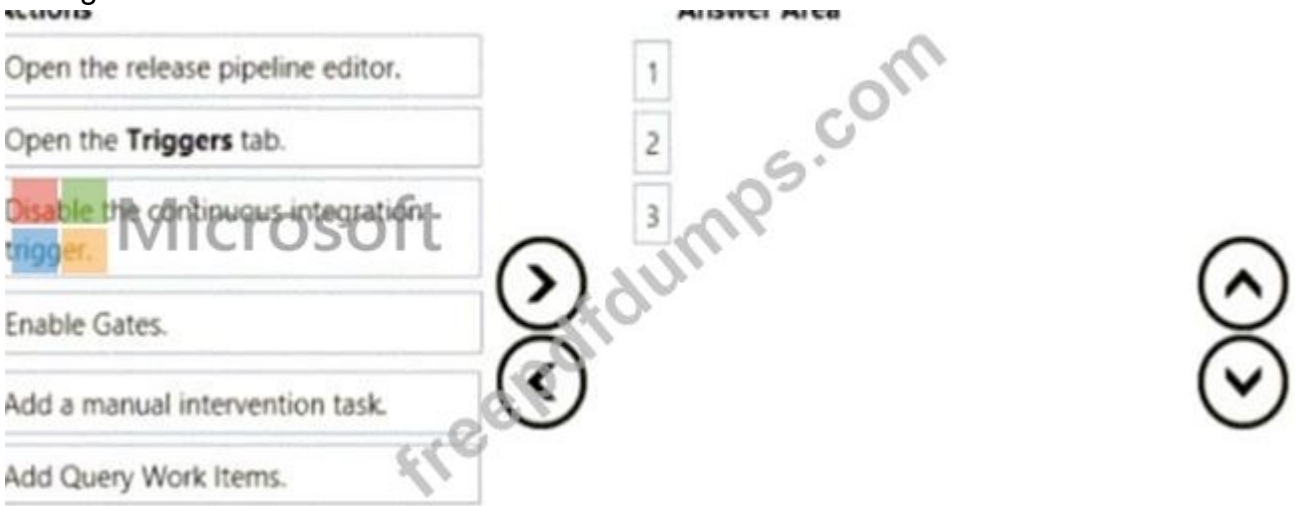
https://docs.microsoft.com/en-us/azure/devops/boards/queries/link-work-items-support-traceability?view=azure-devops&tabs=new-web-form

https://docs.microsoft.com/en-us/visualstudio/releasenotes/tfs2017-relnotes

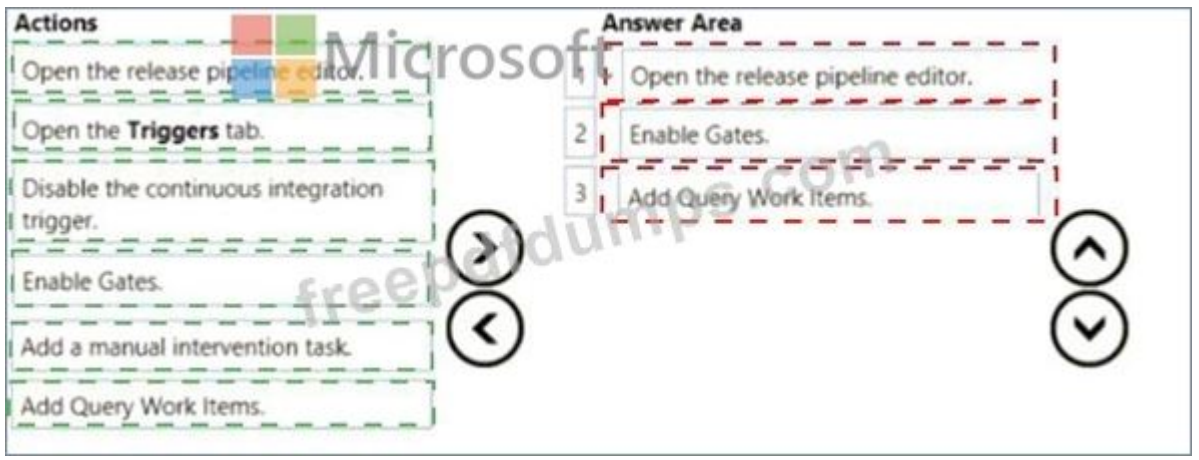
NEW QUESTION: 288

You need to implement Project6.

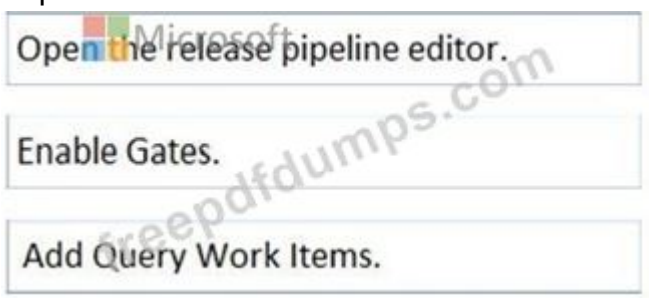
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them m the correct order.



Answer:



Explanation



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

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

Step 1: Open the release pipeline editor.

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

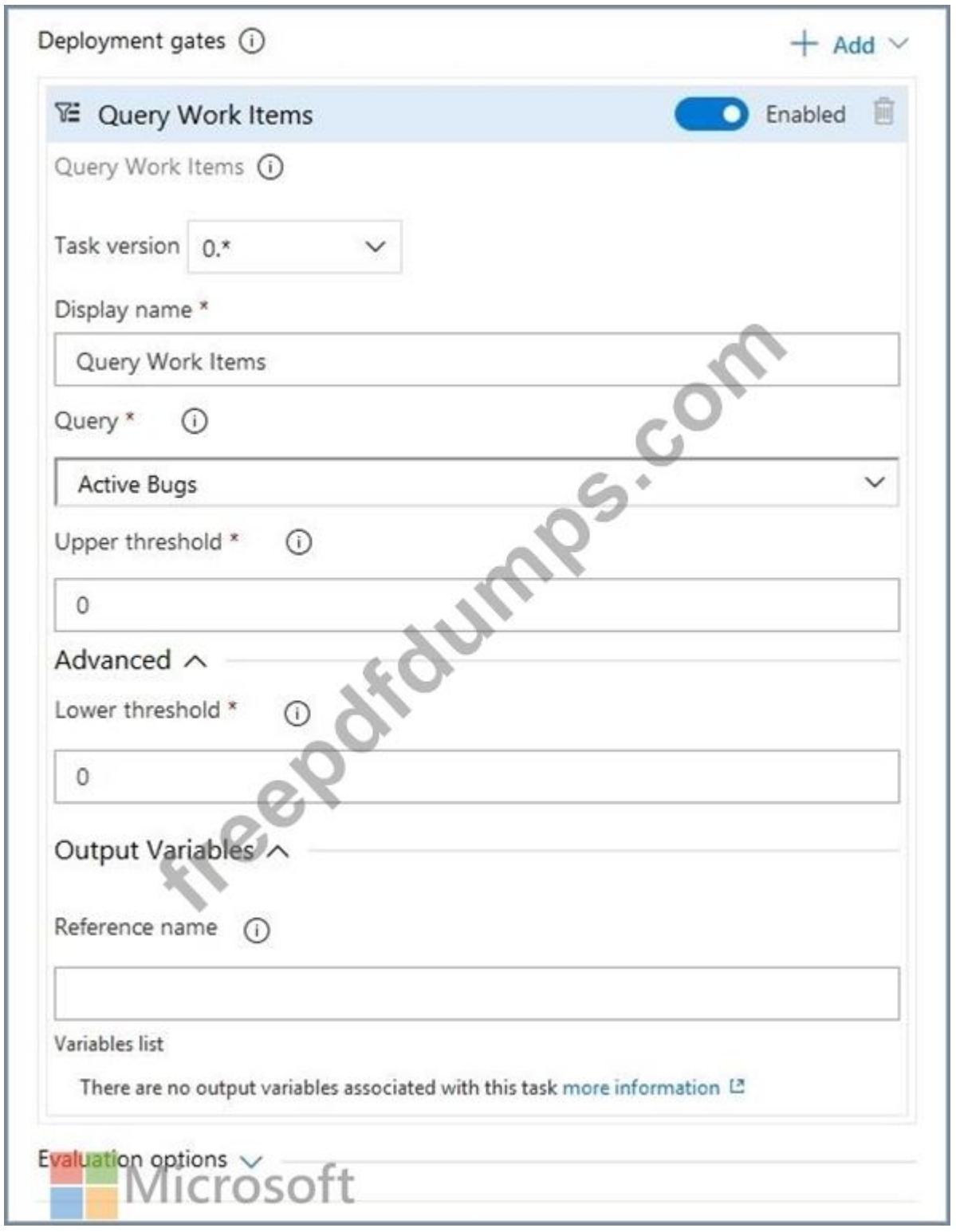
Step 2: Enable Gates.

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

Step 3: Add Query Work items.

Choose + Add and select the Query Work Items gate.

Configure the gate by selecting an existing work item query.

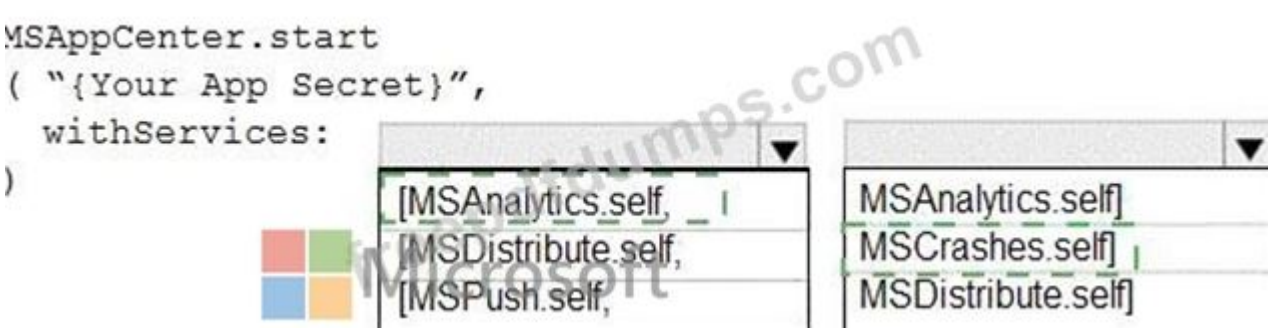


Note: A case for release gate is:
Incident and issues management. Ensure the required status for work items, incidents, and issues. For example, ensure deployment occurs only if no priority zero bugs exist, and validation that there are no active incidents takes place after deployment.
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/release/d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

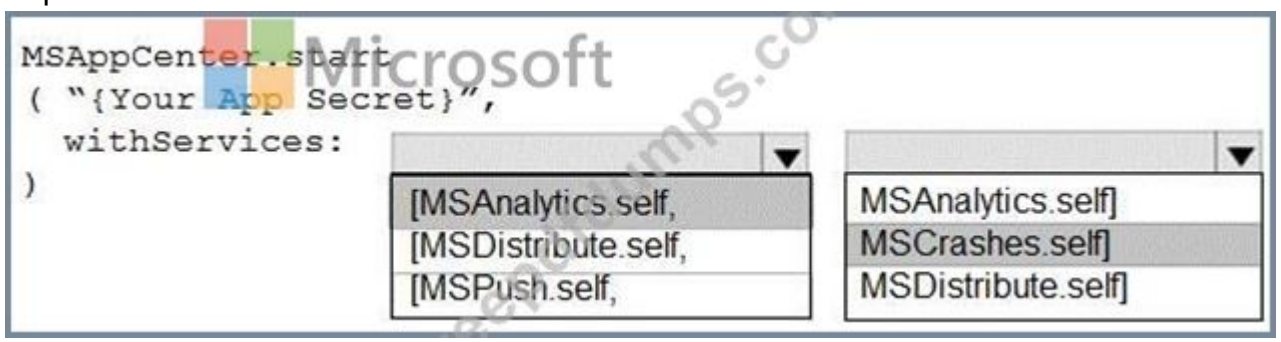
NEW QUESTION: 289
How should you complete the code to initialize App Center in the mobile application? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection a worth one point.

Answer:

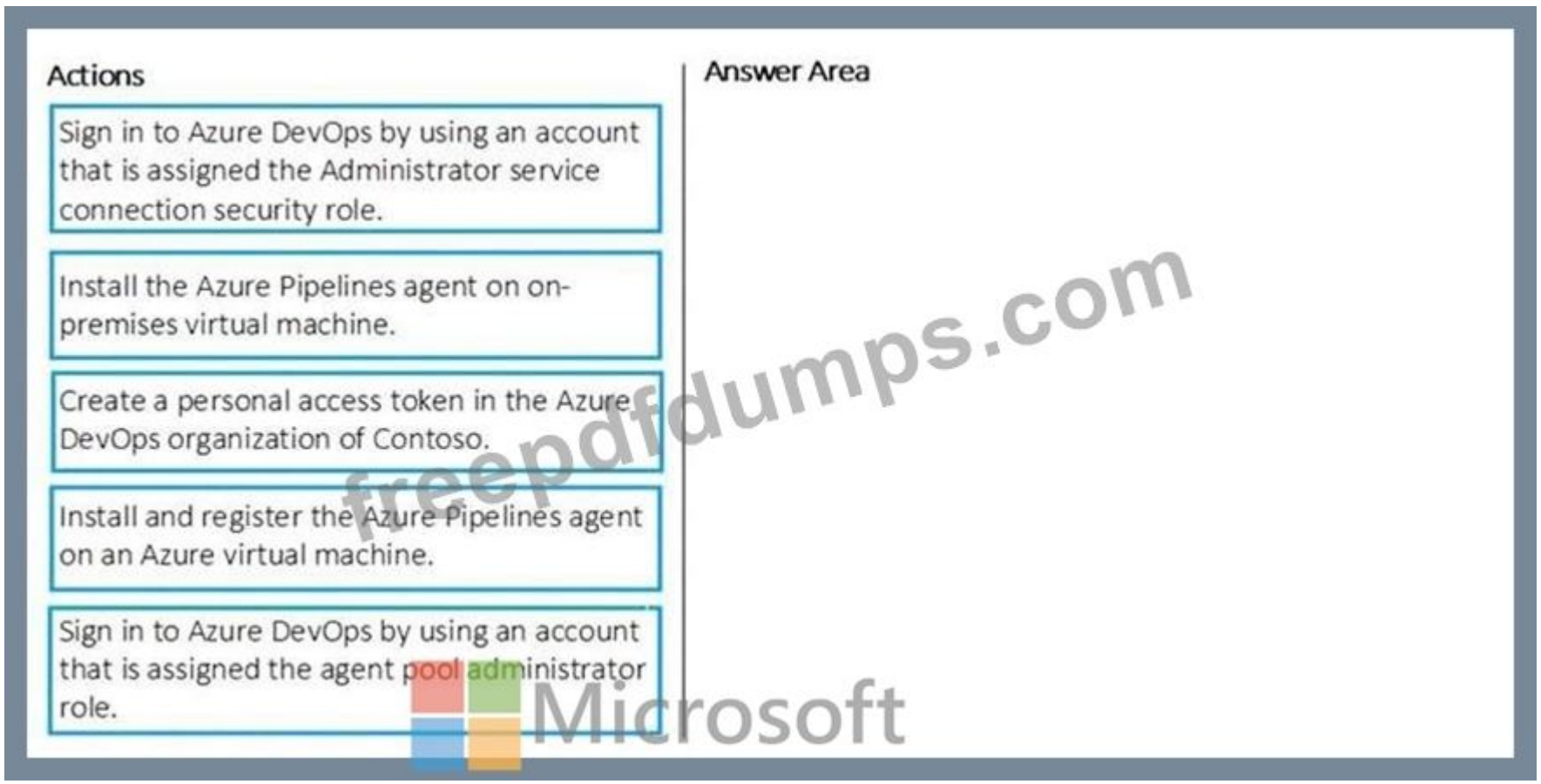


Explanation

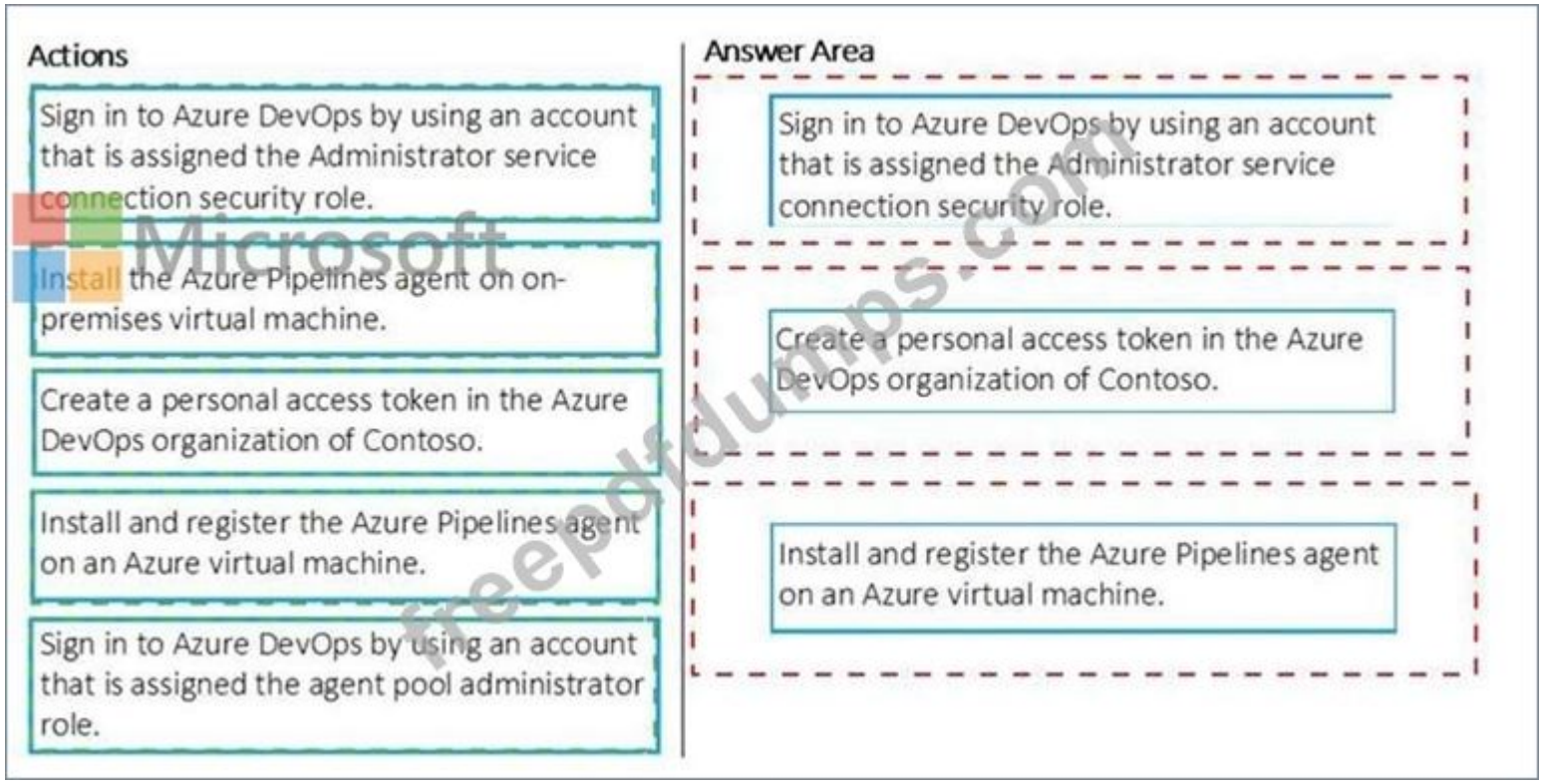


Scenario: Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use.
In order to use App Center, you need to opt in to the service(s) that you want to use, meaning by default no services are started and you will have to explicitly call each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

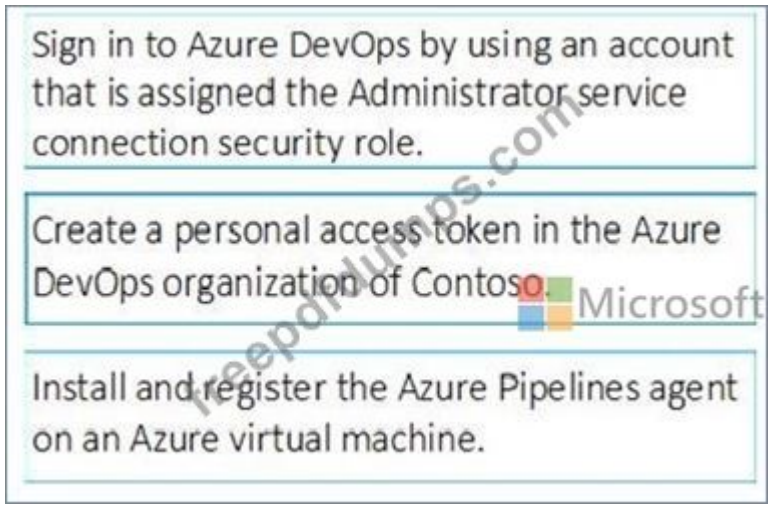
NEW QUESTION: 290
You need to recommend a procedure to implement the build agent for Project1.
Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation



Scenario:

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

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

NEW QUESTION: 291
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a project in Azure DevOps for a new web application.
You need to ensure that when code is checked in, a build runs automatically.
Solution: From the Pre-deployment conditions settings of the release pipeline, you select After stage.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Instead, 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
NEW QUESTION: 292

You have a project Azure DevOps.
You plan to create a build pipeline that will deploy resources by using Azure Resource Manager templates.
The templates will reference secretes stored in Azure Key Vault.
Yu need to ensure that you can dynamically generate the resource ID of the key vault during template deployment.
What should you include in the template? To answer, select eh appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
"resources":[
{
  "apiversion": "2018-05-01",
  "name" : "secrets",
  "type":  [                                  ▼]
             "Microsoft.KeyVault/vaults",
             "Microsoft.Resources/deployment".
             "Microsoft.Subscription/subscriptions".
  "properties":{
     "mode" : "Incremental",
     [                                        ▼] :{
        "deployment"
        "template"
        "templateLink"

contentVersion" : "1.0.0.0",
        "uri" : "[uri(parameters('_artifactsLocation'),
        concat('./nested/sqlserver.json',
        parameters('_artifactsLocationSasToken')))]"
    },
    "parameters":{
        "secret":{
           "reference":{
              "keyVault":{
                 "id": "[resourceId(parameters('vaultSubscription'),
                 parameters('vaultResourceGroupName'),
                 'Microsoft.KeyVault/vaults',
                 parameters('vaultName'))]"
              },
              "secretName": "[parameters('secretName')]"
               }
              }
             }
            }
          }
        ],
```


Answer:

Explanation

NEW QUESTION: 293

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 Application Insights availability test and alert.

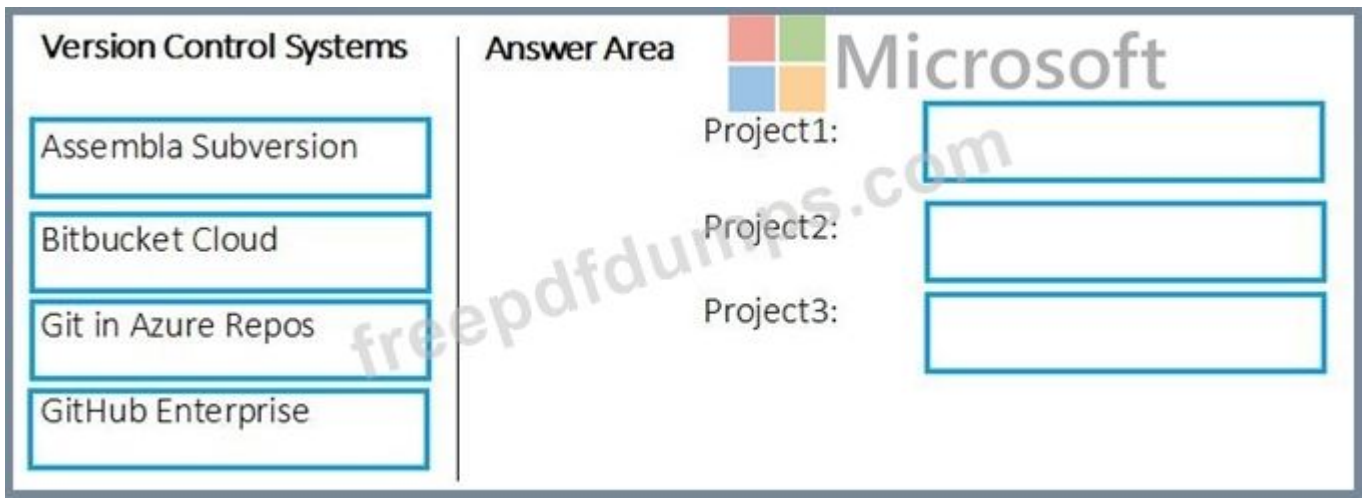
B. Create an Azure Service Health alert for the specific regions.

C. Create an Azure Monitor Availability metric and alert
D. Write an Azure function and deploy the function to the specific regions.
Answer: A (LEAVE A REPLY)
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?
* DependaBot regularly checks dependencies for updates
* If an update is found, DependaBot creates a new branch with this upgrade and Pull Request for approval
* You review the new Pull Request, ensure the tests passed, review the code, and decide if you can merge the change There are three types of Application Insights availability tests:
* URL ping test: a simple test that you can create in the Azure portal.
* Multi-step web test
* Custom Track Availability Tests
Note: After you've deployed your web app/website, you can set up recurring tests to monitor availability and responsiveness. Azure Application Insights sends web requests to your application at regular intervals from points around the world. It can alert you if your application isn't responding, or if it responds too slowly.
You can set up availability tests for any HTTP or HTTPS endpoint that is accessible from the public internet. You don't have to make any changes to the website you're testing. In fact, it doesn't even have to be a site you own. You can test the availability of a REST API that your service depends on.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability#create-a-url-ping-test

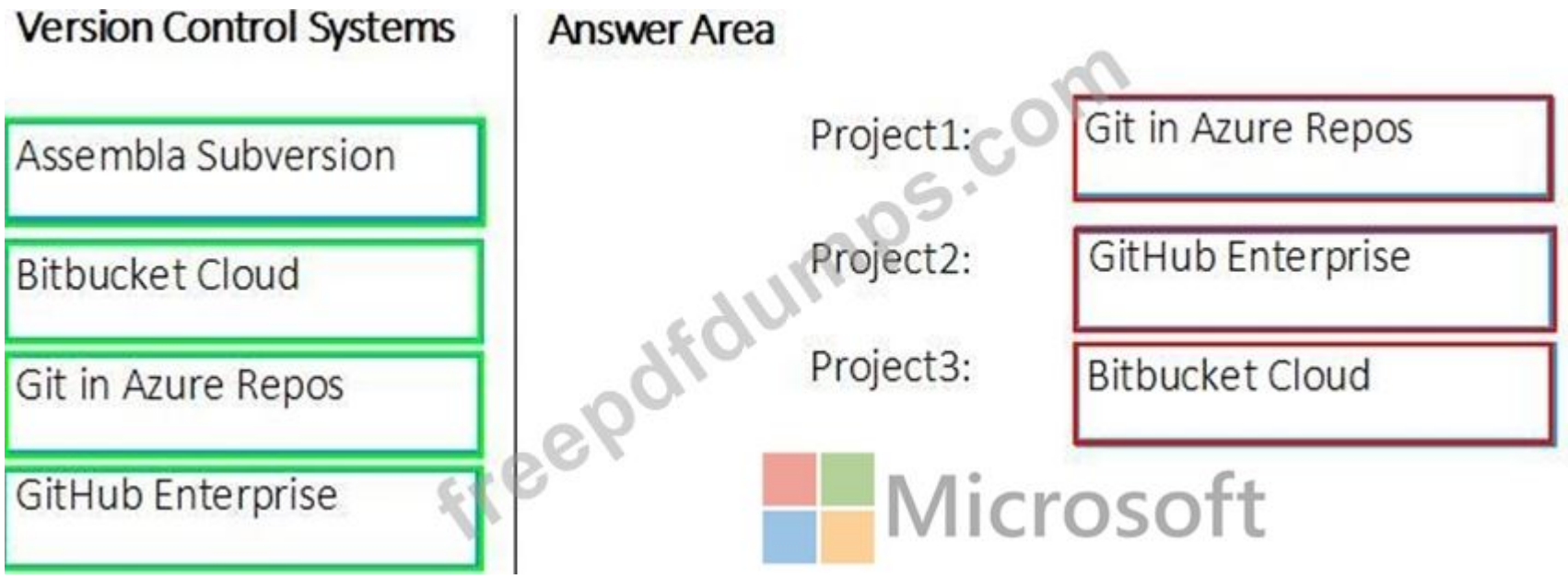
NEW QUESTION: 294
You are configuring Azure Pipelines for three projects in Azure DevOps as shown in the following table.

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.



Answer:



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.

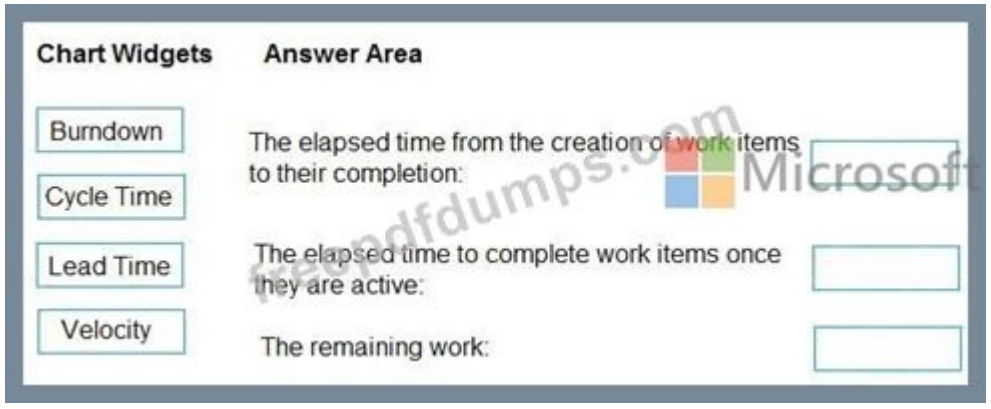
Note: A source control system, also called a version control system, allows developers to collaborate on code and track changes. Source control is an essential tool for multi-developer projects.

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.

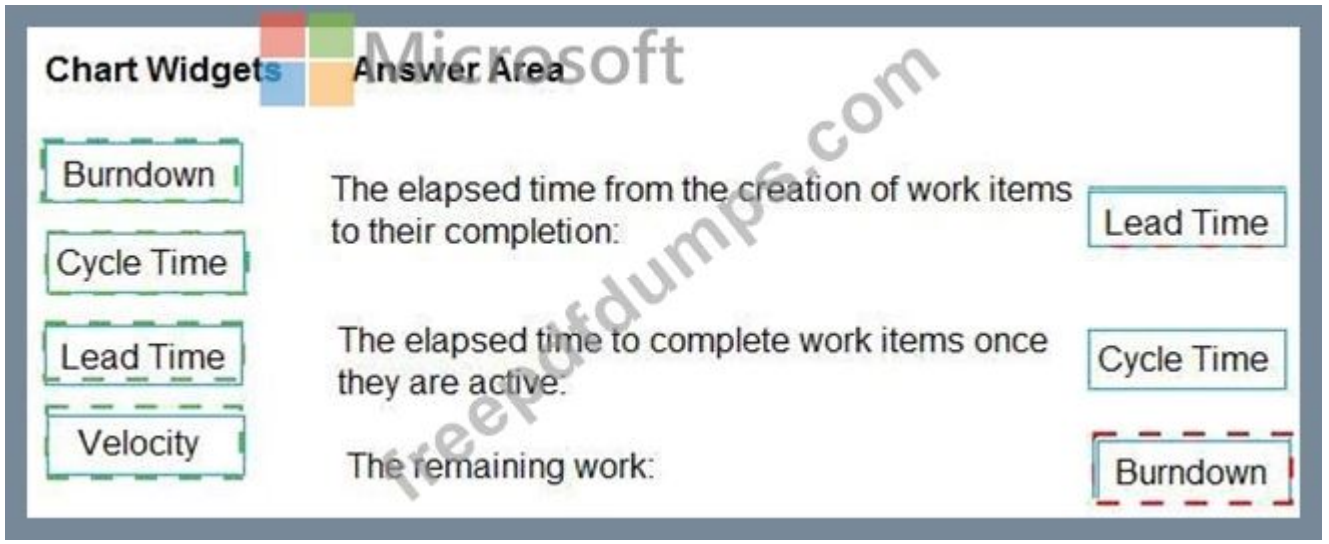
References:
https://www.azuredevopslabs.com/labs/azuredevops/yaml/
https://enterprise.github.com/faq

NEW QUESTION: 295
You are developing an open source solution that uses a GitHub repository.
You create a new public project in Azure DevOps.
You plan to use Azure Pipelines for continuous build. The solution will use the GitHub Checks API.
Which authentication type should you use?
A. a personal access token
B. SAML
C. GitHub App
D. OAuth
Answer: C (LEAVE A REPLY)
Explanation
https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/github?view=azure-devops&tabs=yaml

NEW QUESTION: 296
You need to recommend project metrics for dashboards in Azure DevOps.
Which chart widgets should you recommend for each metric? To answer, drag the appropriate chart widgets to the correct metrics. Each chart widget may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:



Explanation

Box 1: Lead time

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

Box 2: Cycle time

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

Box 3: Burndown

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

NEW QUESTION: 297

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

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

Answer:

See solution below.

Explanation

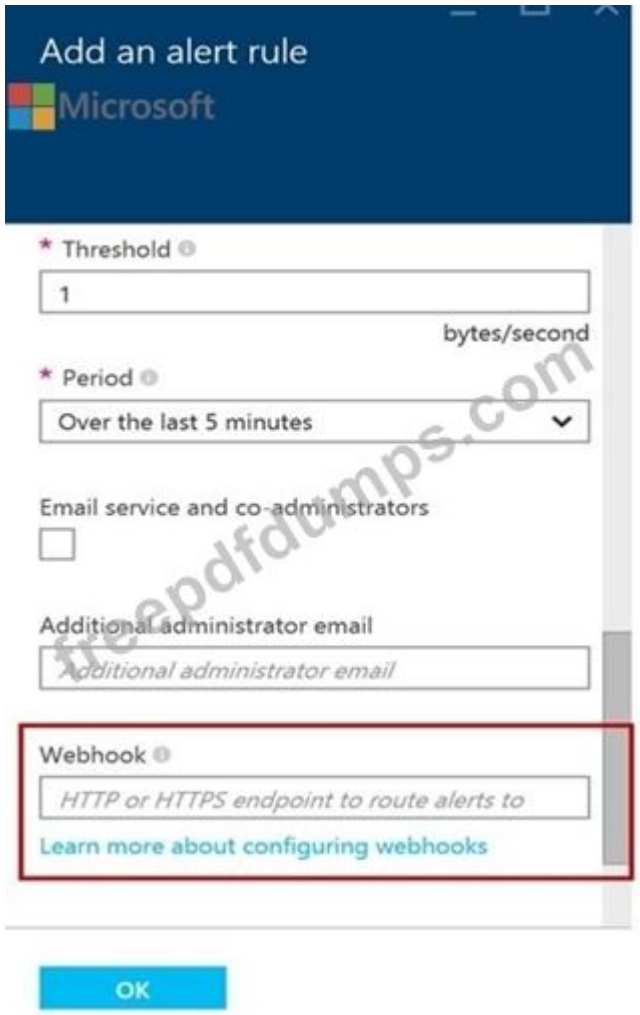
1. Open Microsoft Azure Portal
2. Log into your Azure account and go to App Service and look under Monitoring then you will see Alert.
3. Select Add an alert rule
4. Configure the alert rule as per below and click Ok.

Source: Alert on Metrics

Resource Group: az400-9940427-main

Resource: az400-9940427-main

Threshold: 5
Period: Over the last 5 minutes
Webhook: https://contoso.com/notify



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