AZ-400$^{\text{Q\&As}}$

Designing and Implementing Microsoft DevOps Solutions

Pass Microsoft AZ-400 Exam with 100% Guarantee

QUESTION 1

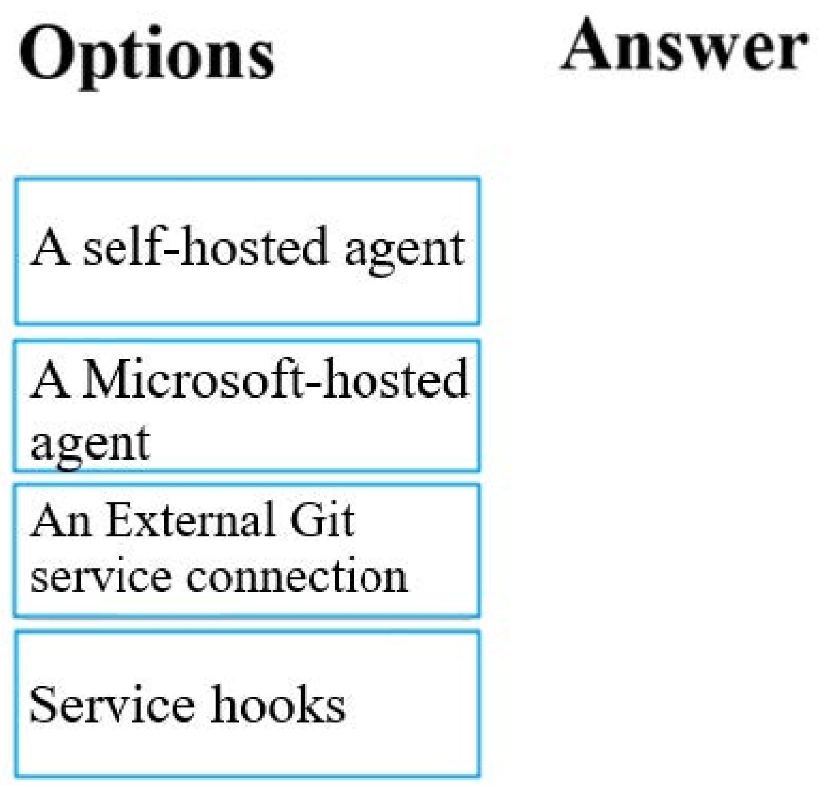
DRAG DROP

You have an on-premises Bitbucket Server with a firewall configured to block inbound Internet traffic. The server is used for Git-based source control.

You intend to manage the build and release processes using Azure DevOps. This plan requires you to integrate Azure DevOps and Bitbucket.

Which of the following will allow for this integration? Answer by dragging the correct options from the list to the answer area.

Select and Place:



Options

Answer

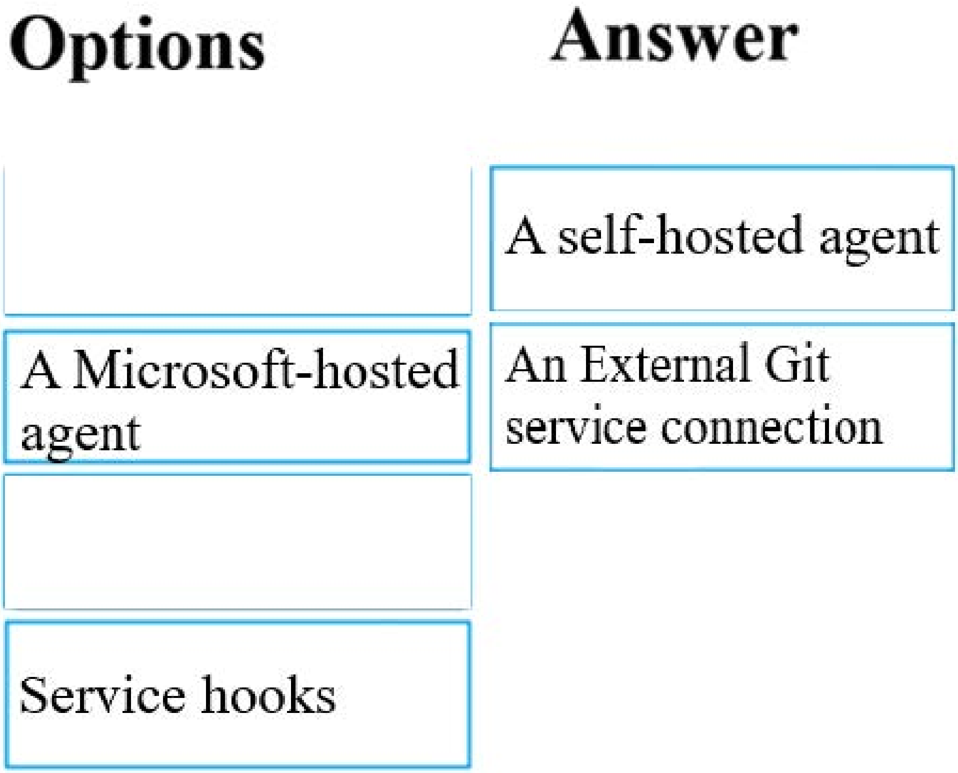
A self-hosted agent

A Microsoft-hosted agent

An External Git service connection

Service hooks

Correct Answer:



Options

Answer

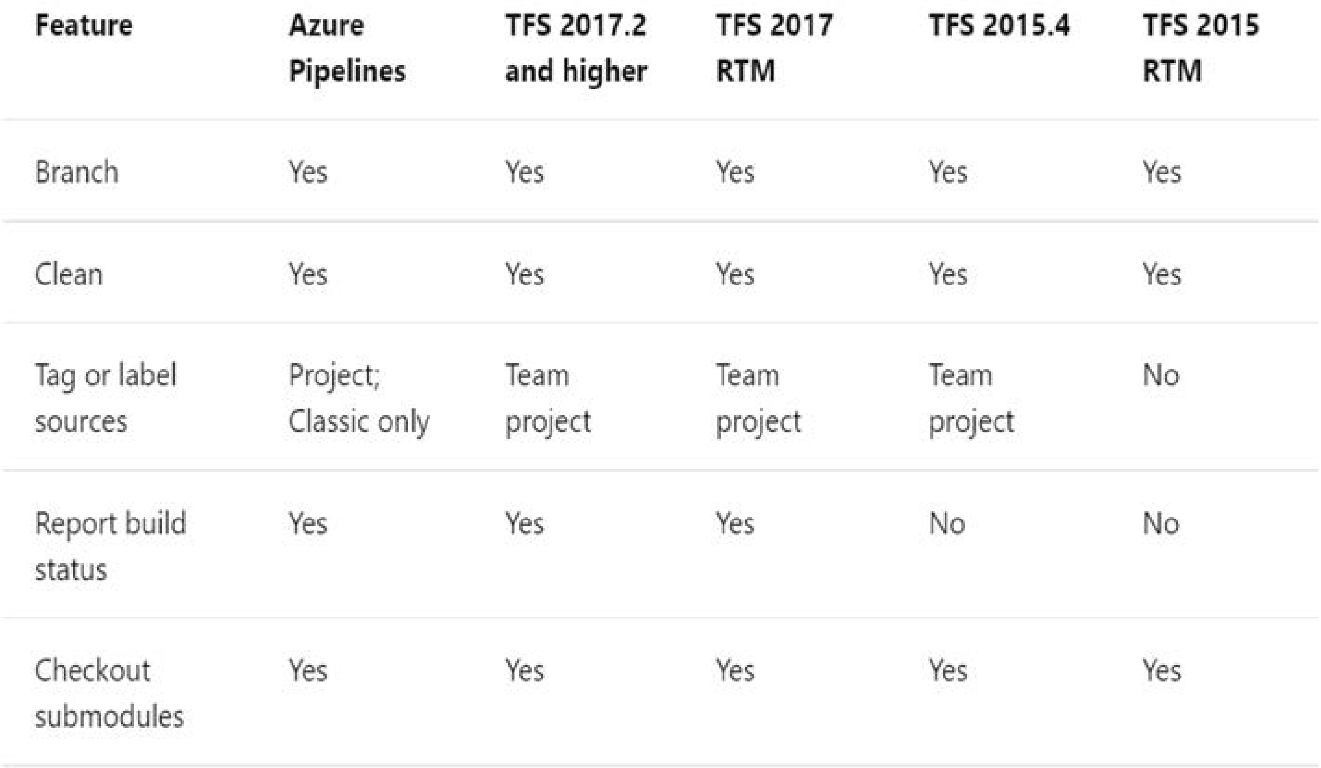
A self-hosted agent

A Microsoft-hosted agent

An External Git service connection

Service hooks

Reference: https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/pipeline-options-for-git



Feature	Azure Pipelines	TFS 2017.2 and higher	TFS 2017 RTM	TFS 2015.4	TFS 2015 RTM
Branch	Yes	Yes	Yes	Yes	Yes
Clean	Yes	Yes	Yes	Yes	Yes
Tag or label sources	Project; Classic only	Team project	Team project	Team project	No
Report build status	Yes	Yes	Yes	No	No
Checkout submodules	Yes	Yes	Yes	Yes	Yes

QUESTION 2

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

You need to create a published wiki in Project1.

What should you do first?

A. Modify the Storage settings of Project1.

B. In Project1, create an Azure DevOps pipeline.

C. In Project1, create an Azure DevOps repository.

D. Modify the Team configuration settings of Project1.

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/devops/project/wiki/publish-repo-to-wiki?view=azure-devopsandtabs=browser

QUESTION 3

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

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

What should you use?

A. Microsoft Visual SourceSafe

B. Code Style

C. Black Duck

D. Jenkins

E. SourceGea

F. OWASP ZAP

Correct Answer: C

Secure and Manage Open Source Software Black Duck helps organizations identify and mitigate open source security, license compliance and code-quality risks across application and container portfolios. Black Duck Hub and its plugin for Team Foundation Server (TFS) allows you to automatically find and fix open source security vulnerabilities during the build process, so you can proactively manage risk. The integration allows you to receive alerts and fail builds when any Black Duck Hub policy violations are met.

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

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

QUESTION 4

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. Create an XAML build service.

B. Create a variable group in Project1.

C. Add a secure file to Project1.

D. Configure the security policy of Contoso.

Correct Answer: D

Before this will work, the build needs permission to access the Azure Key Vault. This can be added in the Azure Portal. Open the Access Policies in the Key Vault and add a new one. Choose the principle used in the DevOps build.
Reference:

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

QUESTION 5

You have a GitHub repository that contains multiple workflows and a secret stored at the environment level.

You need to ensure that the secret can be used by all the workflows.

What should you do first?

A. Recreate the secret at the organization level.

B. Recreate the secret at the repository level.

C. Enable required reviewers.

Correct Answer: B

Encrypted secrets allow you to store sensitive information in your organization, repository, or repository environments.

Secrets are encrypted variables that you create in an organization, repository, or repository environment. The secrets that you create are available to use in GitHub Actions workflows. GitHub uses a libsodium sealed box to help ensure that

secrets are encrypted before they reach GitHub and remain encrypted until you use them in a workflow.

Incorrect:

Not A:

For secrets stored at the organization-level, you can use access policies to control which repositories can use organization secrets. Organization-level secrets let you share secrets between multiple repositories, which reduces the need for

creating duplicate secrets. Updating an organization secret in one location also ensures that the change takes effect in all repository workflows that use that secret.

Reference:

https://docs.github.com/en/actions/security-guides/encrypted-secrets