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

Designing and Implementing Microsoft DevOps Solutions

Pass Microsoft AZ-400 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/az-400.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You use Git for source control.

You enable GitHub code scanning.

You raise a pull request from a non-default branch. In the code scanning output, you receive the following error message: “Analysis not found.”

You need to ensure that the code scanning completes successfully for the pull request.

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 name of the default branch to the on: push specification in the code scanning workflow.

B. Add the name of the non-default branch to the on:push specification in the code scanning workflow.

C. Delete the pull request, and then raise the request again from the default branch.

D. Update the code in the pull request.

E. Add a new workflow for code scanning.

Correct Answer: AD

Explanation:

The solution in this situation is to add the name of the base branch to the on:push and on:pull_request specification in the code scanning workflow on that branch and then make a change that updates the open pull request that you want to

scan.

Note: Reasons for the "Analysis not found" message

After code scanning has analyzed the code in a pull request, it needs to compare the analysis of the topic branch (the branch you used to create the pull request) with the analysis of the base branch (the branch into which you want to merge

the pull request). This allows code scanning to compute which alerts are newly introduced by the pull request, which alerts were already present in the base branch, and whether any existing alerts are fixed by the changes in the pull request.

Initially, if you use a pull request to add code scanning to a repository, the base branch has not yet been analyzed, so it\\'s not possible to compute these details. In this case, when you click through from the results check on the pull request

you will see the "Analysis not found" message.

Reference:

https://docs.github.com/en/github-ae@latest/code-security/code-scanning/automatically-scanning-your-code-for-vulnerabilities-and-errors/setting-up-code-scanning-for-a-repository

QUESTION 2

DRAG DROP

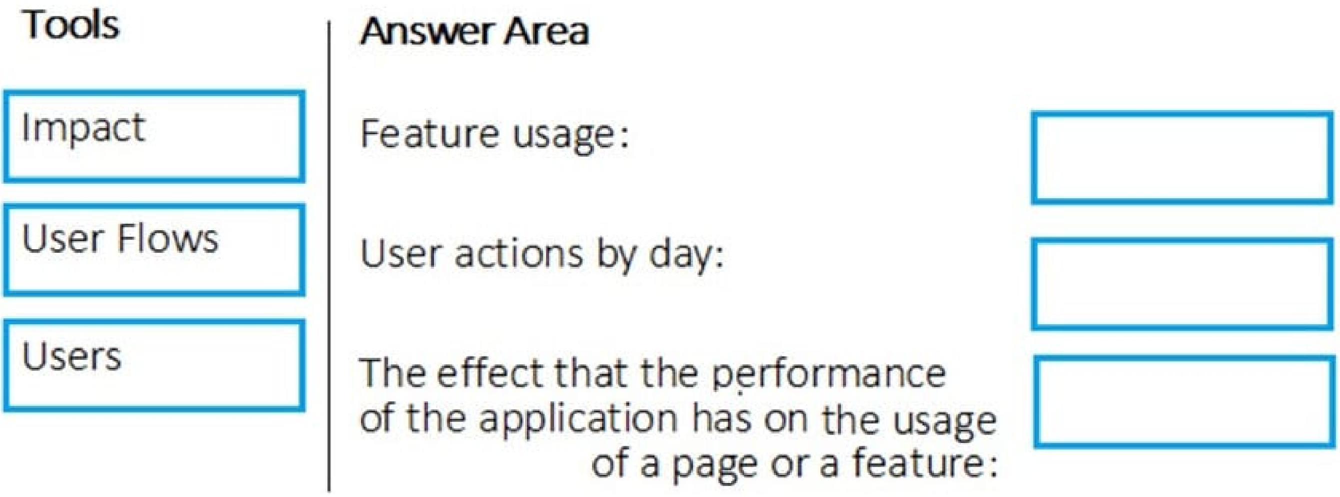
Your company wants to use Azure Application Insights to understand how user behaviors affect an application.

Which application Insights tool should you use to analyze each behavior? To answer, drag the appropriate tools to the correct behaviors. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between

panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Tools

Impact

User Flows

Users

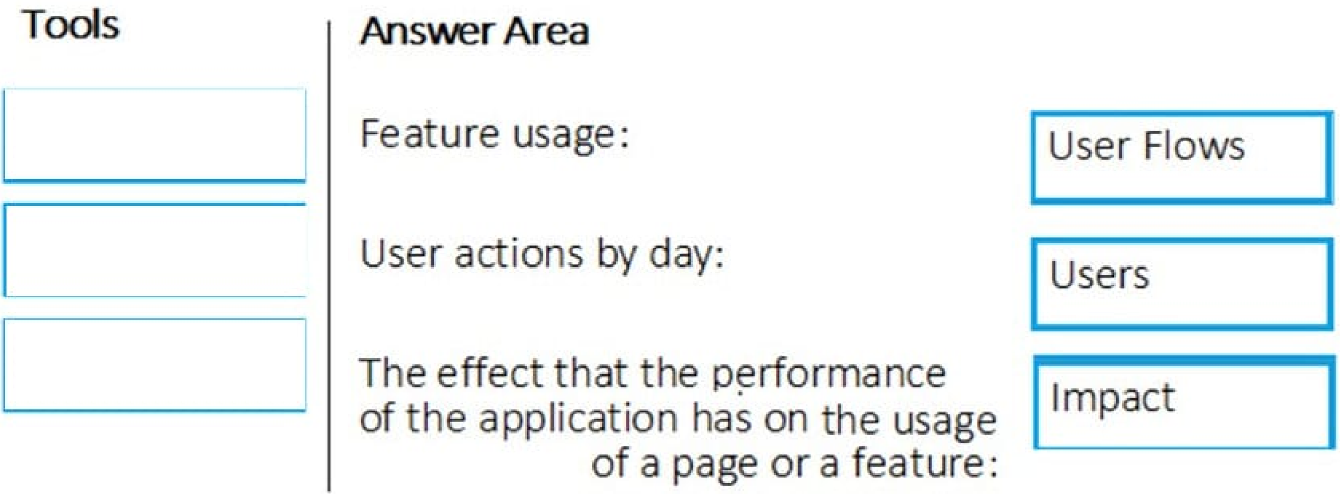
Answer Area

Feature usage:

User actions by day:

The effect that the performance of the application has on the usage of a page or a feature:

Correct Answer:



Tools

Answer Area

Feature usage: User Flows

User actions by day: Users

The effect that the performance of the application has on the usage of a page or a feature: Impact

Box 1: User Flows

The User Flows tool visualizes how users navigate between the pages and features of your site. It\\'s great for answering questions like:

How do users navigate away from a page on your site?

What do users click on a page on your site?

Where are the places that users churn most from your site?

Are there places where users repeat the same action over and over?

Box 2: Users

Box 3: Impact

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-flows

QUESTION 3

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:

1.

Licensing violations

2.

Prohibited libraries

Solution: You implement continuous integration.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.

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

QUESTION 4

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.

Correct Answer: DE

https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-windows?view=azure-devops (Get PAT, run config)

QUESTION 5

DRAG DROP

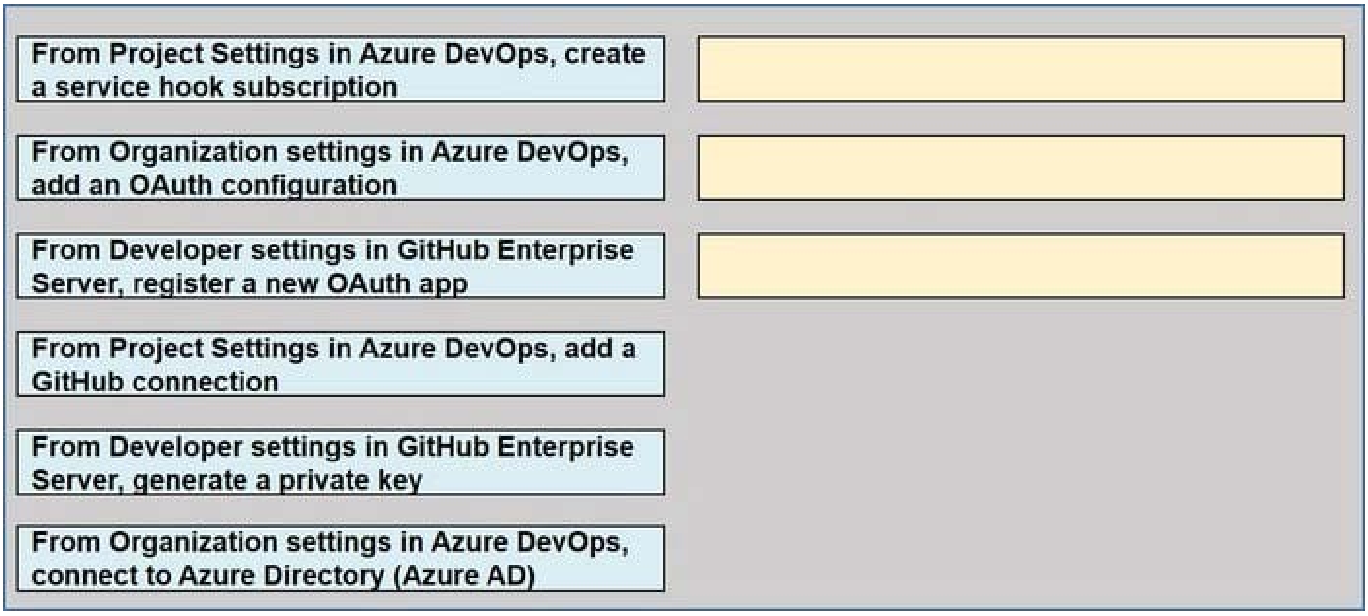
You use GitHub Enterprise Server as a source code repository.

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.

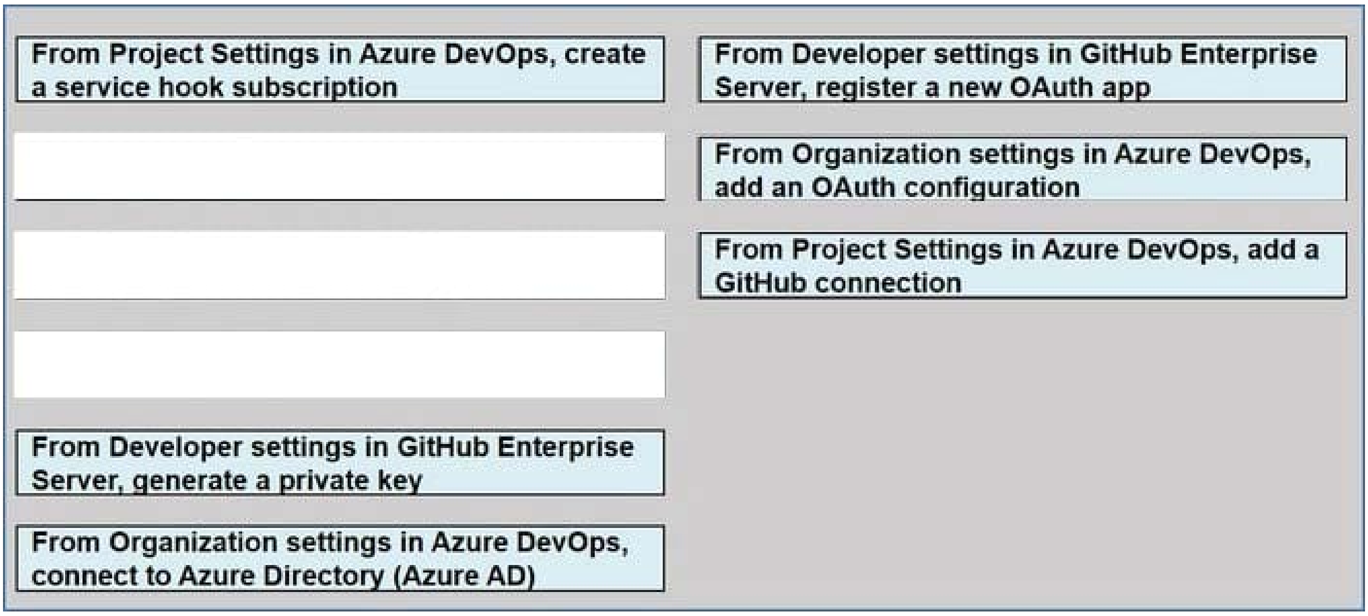
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



From Project Settings in Azure DevOps, create a service hook subscription	
From Organization settings in Azure DevOps, add an OAuth configuration	
From Developer settings in GitHub Enterprise Server, register a new OAuth app	
From Project Settings in Azure DevOps, add a GitHub connection	
From Developer settings in GitHub Enterprise Server, generate a private key	
From Organization settings in Azure DevOps, connect to Azure Directory (Azure AD)	

Correct Answer:



From Project Settings in Azure DevOps, create a service hook subscription	From Developer settings in GitHub Enterprise Server, register a new OAuth app
	From Organization settings in Azure DevOps, add an OAuth configuration
	From Project Settings in Azure DevOps, add a GitHub connection
From Developer settings in GitHub Enterprise Server, generate a private key	
From Organization settings in Azure DevOps, connect to Azure Directory (Azure AD)	

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.