

Exam : AZ-400

Title : Microsoft Azure DevOps Solutions

Vendor : Microsoft

Version : V18.75

NO.1 What should you use to implement the code quality restriction on the release pipeline for the investment planning applications suite?

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

Answer: D

Topic 1, Case Study: 1Overview

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.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 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 existing 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 in detecting failures, rather than always waiting 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 for 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'
```

NO.2 You store source code in a Git repository in Azure repos. You use a third-party continuous integration (CI) tool to control builds.

What will Azure DevOps use to authenticate with the tool?

- A.** certificate authentication
- B.** a personal access token (PAT)
- C.** a Shared Access Signature (SAS) token
- D.** NTLM authentication

Answer: B

Explanation

Personal access tokens (PATs) give you access to Azure DevOps and Team Foundation Server (TFS), without using your username and password directly.

Reference:

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

NO.3 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.

Service connection type:

Azure Resource Manager
Generic service
Team Foundation Server / Azure Pipelines service connection

Authentication/authorization method for the connection:

Azure Active Directory OAuth 2.0
Grant authorization
Managed Service Identity Authentication

Answer:

Service connection type:

Azure Resource Manager
Generic service
Team Foundation Server / Azure Pipelines service connection

Authentication/authorization method for the connection:

Azure Active Directory OAuth 2.0
Grant authorization
Managed Service Identity Authentication

Explanation

Service connection type:

Azure Resource Manager
Generic service
Team Foundation Server / Azure Pipelines service connection

Authentication/authorization method for the connection:

Azure Active Directory OAuth 2.0
Grant authorization
Managed Service Identity Authentication

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>

NO.4 Your company is concerned that when developers introduce open source libraries, it creates licensing compliance issues.

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

What should you use?

- A.** PDM
- B.** OWASPZAP
- C.** WhiteSource
- D.** Jenkins

Answer: C

NO.5 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.

Object to create:

- A build task
- A deployment task
- An artifacts repository



Service to use:

- WhiteSource Bolt
- Bamboo
- CMake
- Chef



Answer:

Object to create:

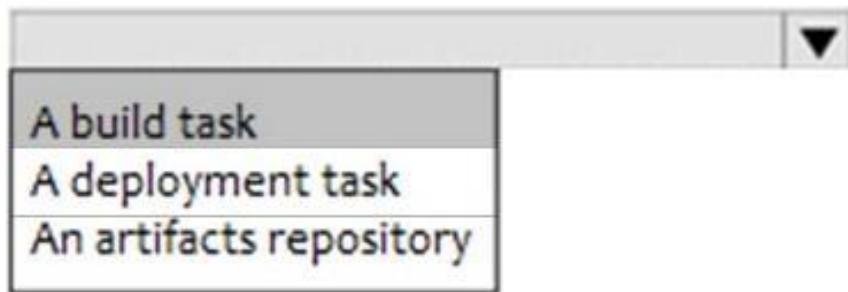
A build task
A deployment task
An artifacts repository

Service to use:

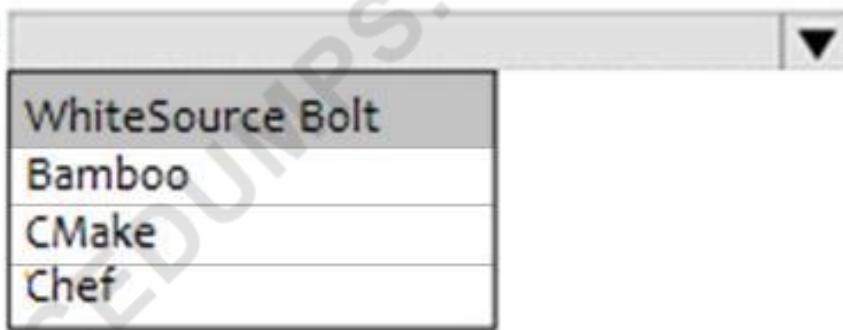
WhiteSource Bolt
Bamboo
CMake
Chef

Explanation

Object to create:



Service to use:



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 definitive database of open source repositories.

References:

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

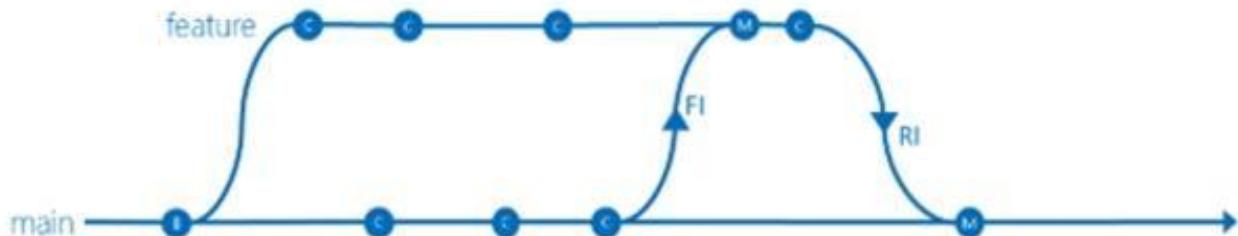
NO.6 Which branching strategy should you recommend for the investment planning applications suite?

- A.** release isolation
- B.** main only
- C.** development isolation

D. feature isolation**Answer:** C

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, 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.

NO.7 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

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

You have a policy stating that approvals must occur within eight hours.

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

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

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

Does this meet the goal?

A. Yes

B. NO

Answer: B

NO.8 You have a GitHub repository.

You create a new repository in Azure DevOps.

You need to recommend a procedure to clone the repository from GitHub to Azure DevOps.

What should you recommend?

A. Create a pull request.

B. Create a webhook.

C. Create a service connection for GitHub.

D. From Import a Git repository, click Import.

E. Create a personal access token in Azure DevOps.

Answer: D

Explanation

You can import an existing Git repo from GitHub, Bitbucket, GitLab, or other location into a new or

empty existing repo in your project in Azure DevOps.

Import into a new repo

- * 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>

NO.9 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.

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

Answer:

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

Explanation

Answer Area

- 1 Create a PowerShell configuration file.
- 2 Load the file to Azure Blob storage.
- 3 Configure the Custom Script Extension on the virtual machines.

Step 1: Create a PowerShell configuration file

You create a simple PowerShell DSC configuration file.

Step 2: Load the file to Azure Blob storage

Package and publish the module to a publically accessible blob container URL Step 3: Configure the Custom Script Extension on the virtual machines.

The Custom Script Extension downloads and executes scripts on Azure virtual machines.

Reference:

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

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

NO.10 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 Microsoft-hosted agent pool running a Linux image.

Include the Java Tool Installer task in the build pipeline.

Does this meet the goal?

A. Yes

B. No

Answer: B

NO.11 Your company is building a new solution in Java.

The company currently uses a SonarQube server to analyze the code of .NET solutions.

You need to analyze and monitor the code quality of the Java solution.

Which task types should you add to the build pipeline?

A. Octopus

B. Chef

C. Maven

D. Grunt

Answer: A

NO.12 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: C

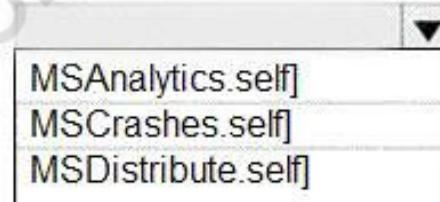
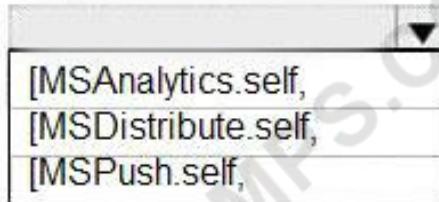
Explanation

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

NO.13 How should you complete the code to initialize App Center in the mobile application? To answer, select the appropriate options in the answer area.

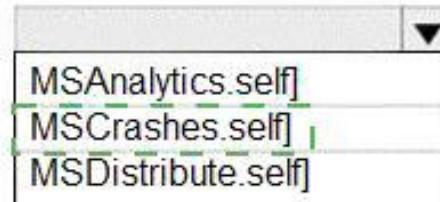
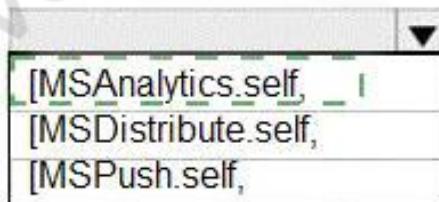
NOTE: Each correct selection a worth one point.

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



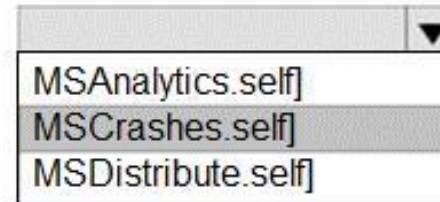
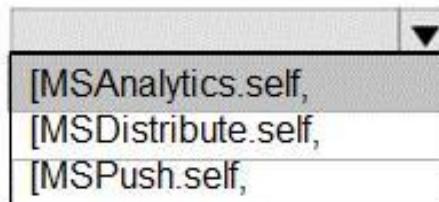
Answer:

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



Explanation

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



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>

NO.14 You plan to share packages that you wrote, tested, validated, and deployed by using Azure Artifacts.

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

What should you use?

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

Answer: D

Explanation

Views enable you to share subsets of the NuGet, npm, Maven, Python and Universal Packages package-versions in your feed with consumers. A common use for views is to share package versions that have been tested, validated, or deployed but hold back packages still under development and packages that didn't meet a quality bar.

<https://docs.microsoft.com/en-us/azure/devops/artifacts/concepts/views?view=azure-devops>

NO.15 You use Azure SQL Database Intelligent Insights and Azure Application Insights for monitoring.

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

Which Query language should you use?

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

Answer: C

Explanation

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

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

NO.16 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.** GitHubApp
- B.** OAuth
- C.** personal access token (PAT)
- D.** Azure Active Directory (Azure AD)

Answer: A

Explanation

GitHub App uses the Azure Pipelines identity.

Reference:

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

NO.17 Your company has a hybrid cloud between Azure and Azure Stack.

The company uses Azure DevOps for its CI/CD pipelines. Some applications are built by using Erlang and Hack.

You need to ensure that Erlang and Hack are supported as part of the build strategy across the hybrid cloud.

The solution must minimize management overhead.

What should you use to execute the build pipeline?

- A.** AzureDevOps self-hosted agents on Azure DevTest Labs virtual machines.
- B.** AzureDevOps self-hosted agents on virtual machine that run on Azure Stack
- C.** AzureDevOps self-hosted agents on Hyper-V virtual machines
- D.** a Microsoft-hosted agent

Answer: B

Explanation

Azure Stack offers virtual machines (VMs) as one type of an on-demand, scalable computing resource. You can choose a VM when you need more control over the computing environment.

References: <https://docs.microsoft.com/en-us/azure/azure-stack/user/azure-stack-compute-overview>

NO.18 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: B

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>

NO.19 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.

count()

makelist(EventID)

makeset(EventID)

mv-expand

project

render

summarize

Answer Area

```
Event
| where TimeGenerated > ago(12h)
| order by TimeGenerated desc
|     Value           Value
|     -----           -----
|     by Computer
```

Answer:

count()

makelist(EventID)

makeset(EventID)

mv-expand

project

render

summarize

Answer Area

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

Explanation

Event

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

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>

NO.20 Your company is building a new web application.

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

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

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

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

Developers:

A dropdown menu with the label "Developers:" to its left. The menu contains two items: "Basic" and "Stakeholder".

Pilot users:

A dropdown menu with the label "Pilot users:" to its left. The menu contains two items: "Basic" and "Stakeholder".

Answer:

Developers:

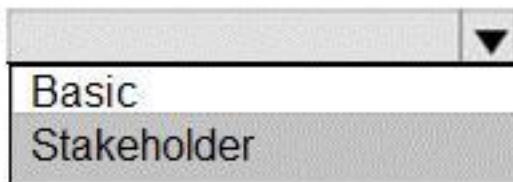
A dropdown menu with the label "Developers:" to its left. The item "Basic" is highlighted with a green dashed border.

Pilot users:

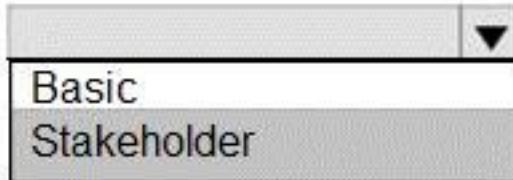
A dropdown menu with the label "Pilot users:" to its left. The item "Stakeholder" is highlighted with a green dashed border.

Explanation

Developers:



Pilot users:



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>

NO.21 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

Explanation

There are three types of Application Insights availability tests:

- * URL ping test: a simple test that you can create in the Azure portal.
- * Multi-step web test
- * Custom Track Availability Tests

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

You can set up availability tests for any HTTP or HTTPS endpoint that is accessible from the public internet.

You don't have to make any changes to the website you're testing. In fact, it doesn't even have to be

a site you own. You can test the availability of a REST API that your service depends on.

Reference:

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

NO.22 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.

D18912E1457D5D1DDCBD40AB3BF70D5D

- 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

Explanation

BE: An app deployed to Azure can take advantage of Managed identities for Azure resources, which allows the app to authenticate with Azure Key Vault using Azure AD authentication without credentials (Application ID and Password/Client Secret) stored in the app.

- * Select Add Access Policy.
- * Open Secret permissions and provide the app with Get and List permissions.
- * Select Select principal and select the registered app by name. Select the Select button.
- * Select OK.
- * Select Save.
- * Deploy the app.

References:

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

<https://docs.microsoft.com/en-us/azure/key-vault/general/tutorial-net-virtual-machine>

NO.23 Your company wants to use Azure Application Insights to understand how user behaviors affect an application.

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

NOTE: Each correct selection is worth one point.

Tools

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:

Answer:**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:

Explanation**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>

NO.24 You have several apps that use an Azure SQL Database named db1.

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

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

Answer:

See solution below.

Explanation

1. To enable automatic tuning on a single database, navigate to the database in the Azure portal and select Automatic tuning.

OPTION	DESIRED STATE	CURRENT STATE
FORCE PLAN	ON OFF INHERIT	ON Inherited from server
CREATE INDEX	ON OFF INHERIT	ON Inherited from server
DROP INDEX	ON OFF INHERIT	ON Forced by user

2. Select the automatic tuning options you want to enable and select Apply.

Note: Individual automatic tuning settings can be separately configured for each database. You can manually configure an individual automatic tuning option, or specify that an option inherits its settings from the server.

Reference:

<https://docs.microsoft.com/en-us/azure/sql-database/automatic-tuning-enable>

NO.25 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 must meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

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

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

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

Does this meet the goal?

A. Yes

B. NO

Answer: A

Explanation

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

References:

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

NO.26 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You manage a project in Azure DevOps.

You need to prevent the configuration of the project from changing over time.

Solution: Implement Continuous Integration for the project.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead implement Continuous Assurance for the project.

Reference:

<https://azsk.azurewebsites.net/04-Continuous-Assurance/Readme.html>

NO.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.

Actions Commands Cmdlets Statements

Run Code Analysis

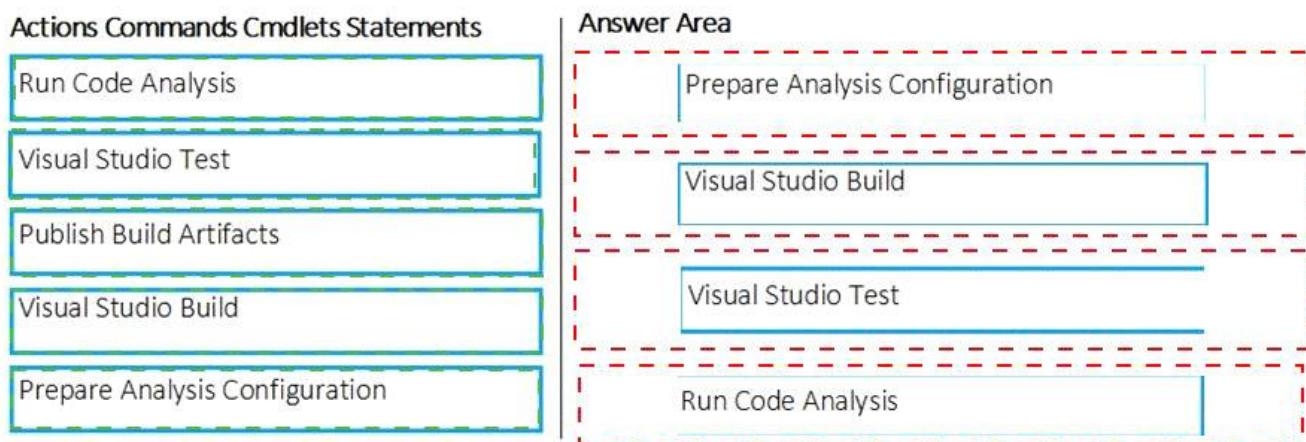
Visual Studio Test

Publish Build Artifacts

Visual Studio Build

Prepare Analysis Configuration

Answer Area

Answer:**Explanation**

Prepare Analysis Configuration

Visual Studio Build

Visual Studio Test

Run Code Analysis

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:

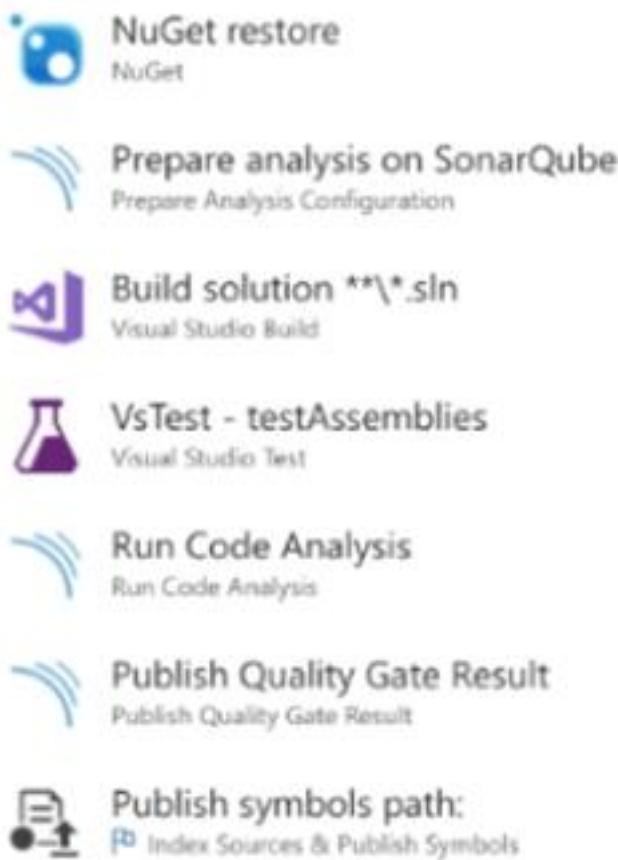
Run Code Analysis task after the Visual Studio Test task.

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>

NO.28 You have the following Azure policy.

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

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

Answer: A

NO.29 Your company is concerned that when developers introduce open source Libraries, it creates licensing compliance issues.

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

What should you use?

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

Answer: C

Explanation

Secure and Manage Open Source Software

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

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

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

References:

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

NO.30 You have a project in Azure DevOps named Contoso App that contains pipelines in Azure Pipelines for GitHub repositories. You need to ensure that developers receive Microsoft Teams notifications when there are failures in a pipeline of Contoso App. What should you run in Teams? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Actions

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



Answer Area

- 1 Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1.
- 2 Run the Import-AzureRmAutomationDscConfiguration Azure PowerShell cmdlet.
- 3 Run the Start-AzureRmAutomationDscCompilationJob Azure PowerShell cmdlet.



Explanation



Box 1: subscribe

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

@azure pipelines subscribe [project url]

Box 2: <https://dev.azure.com/contoso/contoso-app/>

Subscribe to a pipeline or all pipelines in a project to receive notifications:

@azure pipelines subscribe [pipeline url/ project url]

NO.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 need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

- * The builds must access an on-premises dependency management system.
- * The build outputs must be stored as Server artifacts in Azure DevOps.
- * The source code must be stored in a Git repository in Azure DevOps.

Solution: Configure an Octopus Tentacle on an on-premises machine. Use the Package Application task in the build pipeline.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation

Octopus Deploy is an automated deployment server that makes it easy to automate deployment of ASP.NET web applications, Java applications, NodeJS application and custom scripts to multiple environments.

Octopus can be installed on various platforms including Windows, Mac and Linux. It can also be integrated with most version control tools including VSTS and GIT.

When you deploy software to Windows servers, you need to install Tentacle, a lightweight agent service, on your Windows servers so they can communicate with the Octopus server.

When defining your deployment process, the most common step type will be a package step. This step deploys your packaged application onto one or more deployment targets.

When deploying a package you will need to select the machine role that the package will be deployed to.

References:

<https://octopus.com/docs/deployment-examples/package-deployments>

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

NO.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.

The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.

You need to recommend changes to reduce the accumulated technical debt.

Solution: You recommend reducing the code coupling and the dependency cycles?

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead reduce the code complexity.

Note: Technical debt is the accumulation of sub-optimal technical decisions made over the lifetime of an application. Eventually, it gets harder and harder to change things: it's the 'sand in the gears' that sees IT initiatives grind to a halt.

Reference:

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

<https://www.devopsgroup.com/blog/five-ways-devops-helps-with-technical-debt/>

NO.33 You have an Azure DevOps project named Project1 and an Azure subscription named Sub1. You need to prevent releases from being deployed unless the releases comply with the Azure Policy rules assigned to Sub1.

What should you do in the release pipeline of Project1?

A. Create a pipeline variable.

B. Add a deployment gate.

C. Configure a deployment trigger.

D. Modify the Deployment queue settings.

Answer: B

Explanation

You can check policy compliance with gates.

You can extend the approval process for the release by adding a gate. Gates allow you to configure automated calls to external services, where the results are used to approve or reject a deployment.

You can use gates to ensure that the release meets a wide range of criteria, without requiring user intervention.

Reference:

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

NO.34 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

- * The builds must access an on-premises dependency management system.
- * The build outputs must be stored as Server artifacts in Azure DevOps.
- * The source code must be stored in a Git repository in Azure DevOps.

Solution: Install and configure a self-hosted build agent on an on-premises machine. Configure the build pipeline to use the Default agent pool. Include the Java Tool Installer task in the build pipeline. Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead use Octopus Tentacle.

References:

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

NO.35 You have 50 Node.js-based projects that you scan by using WhiteSource. Each project includes Package.json, Package-lock.json, and Npm-shrinkwrap.json files.

You need to minimize the number of libraries reports by WhiteSource to only the libraries that you explicitly reference.

What should you do?

- A.** Configure the File System Agent plug in.
- B.** Delete Package lock.json.
- C.** Configure the Artifactory plug-in.
- D.** Add a devDependencies section to Package-lock.json.

Answer: D

Explanation

Separate Your Dependencies

Within your package.json file be sure you split out your npm dependencies between devDependencies and (production) dependencies. The key part is that you must then make use of the --production flag when installing the npm packages. The --production flag will exclude all packages defined in the devDependencies section.

References:

<https://blogs.msdn.microsoft.com/visualstudioalmrangers/2017/06/08/manage-your-open-source-usage-and-secu>

NO.36 You plan to implement a CI/CD strategy for an Azure Web App named az400-11566895-main.

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

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

Answer:

See solution below.

Explanation

Add a slot

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

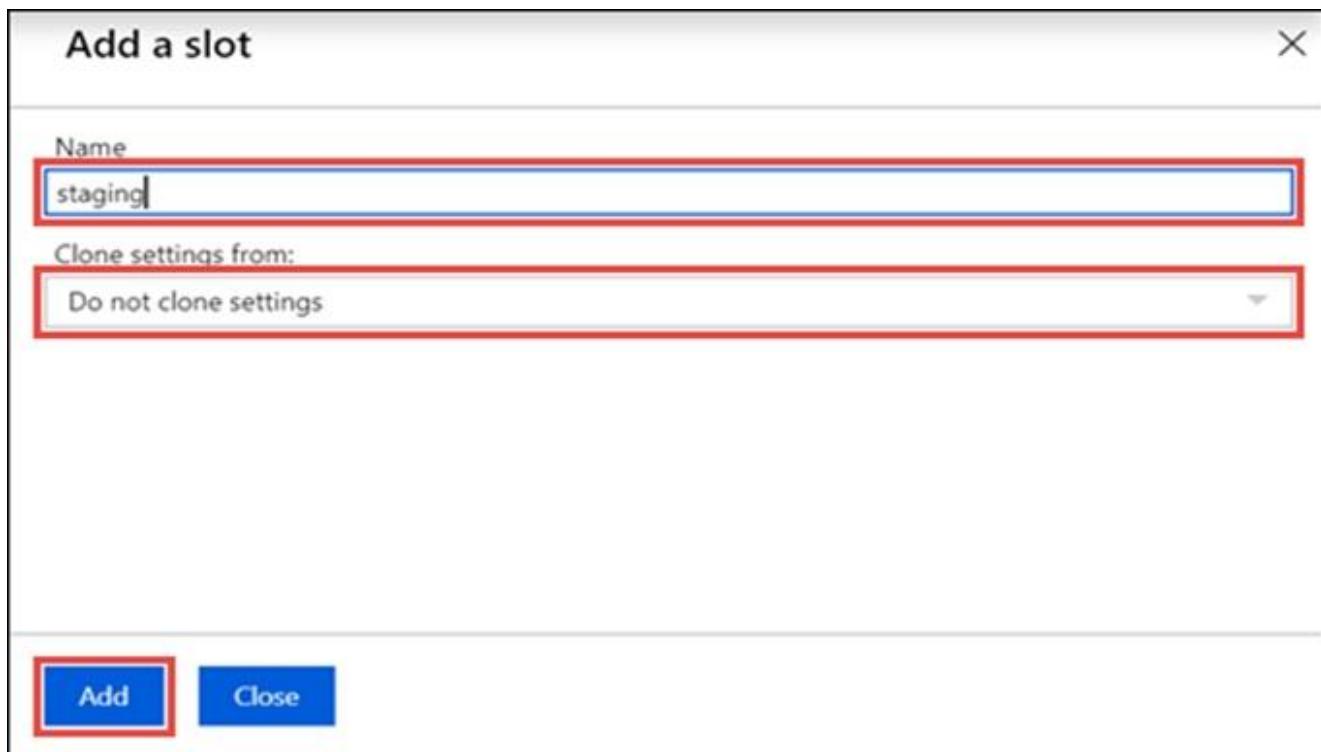
The screenshot shows the Microsoft Azure portal interface. In the top navigation bar, the URL is https://portal.azure.com/. A search bar contains the text 'app services'. Below the search bar, a sidebar titled 'Azure services' includes options like 'Create a resource', 'Resource groups', and 'Recent resources'. The 'Recent resources' section lists three items: 'myFirstAzureWebA', 'WebApplicationAS', and 'cs4316e81020662x'. The main content area is titled 'Services' and shows a list of services under 'All 60 results'. The 'App Services' item is highlighted with a red box. Other listed services include Function App, Service Health, App Service Certificates, App Service Domains, App Service Environments, App Service plans, Lab Services, Media services, Bot Services, and Marketplace.

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

The screenshot shows the 'my-demo-app - Deployment slots' blade. On the left, a sidebar lists various app service management options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Deployment (with 'Quickstart' and 'Deployment slots' selected), Deployment Center, Settings, and Configuration. The main content area is titled 'Deployment Slots' and contains a message: 'You haven't added any deployment slots. Click here to get started.' Below this is a table showing the current deployment slots:

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

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.

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

Reference:

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

NO.37 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You need to ensure that when code is checked in, a build runs automatically.

Solution: From the Pre-deployment conditions settings of the release pipeline, you select Batch changes while a build is in progress.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Use a Pull request trigger.

Note: Batch changes

Select this check box if you have a lot of team members uploading changes often and you want to reduce the number of builds you are running. If you select this option, when a build is running, the system waits until the build is completed and then queues another build of all changes that have not yet been built.

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

NO.38 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.

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



Answer:

Actions
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 Active Directory (Azure AD).

Answer Area
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+



Explanation

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.

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>

NO.39 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: A D

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 File based logs IIS logs .NET app logs Crash dumps Agent diagnostics logs	Event Logs ETW events Performance File based logs IIS logs Insights and solutions Other services	Event Logs Performance File based logs IIS logs Insights and solutions Other services	Process dependencies Network connection metrics
Data sent to	Azure Monitor Logs Azure Monitor Metrics	Azure Storage Azure Monitor Metrics Event Hub	Azure Monitor Logs	Azure Monitor Logs (through Log Analytics agent)

Reference:

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

NO.40 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: B

Explanation

<https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops&tabs=browser#faq>

NO.41 You have an Azure DevOps project that contains a build pipeline. The build pipeline uses approximately 50 open source libraries.

You need to ensure that all the open source libraries comply with your company's licensing standards.

Which service should you use?

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

Answer: C

Explanation

WhiteSource provides WhiteSource Bolt, a lightweight open source security and management solution developed specifically for integration with Azure DevOps and Azure DevOps Server.

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

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

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

Reference:

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

NO.42 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

Explanation

WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build

tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.

Reference:

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

NO.43 You need to use Azure Automation Sure Configuration to manage the ongoing consistency of virtual machine configurations.

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

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

Actions

Answer Area

Onboard the virtual machines to Azure Automation State Configuration.

Check the compliance status of the node.

Create a management group.

Assign the node configuration.



Compile a configuration into a node configuration.

Upload a configuration to Azure Automation State Configuration.

Assign tags to the virtual machines.

Answer:

Actions	Answer Area
Onboard the virtual machines to Azure Automation State Configuration.	Assign the node configuration.
Check the compliance status of the node.	Upload a configuration to Azure Automation State Configuration.
Create a management group.	Compile a configuration into a node configuration.
Assign the node configuration.	 
Compile a configuration into a node configuration.	Onboard the virtual machines to Azure Automation State Configuration.
Upload a configuration to Azure Automation State Configuration.	Check the compliance status of the node.
Assign tags to the virtual machines.	

Explanation

Assign the node configuration.

Upload a configuration to Azure Automation State Configuration.

Compile a configuration into a node configuration.

Onboard the virtual machines to Azure Automation State Configuration.

Check the compliance status of the node.

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>

NO.44 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You manage a project in Azure DevOps.

You need to prevent the configuration of the project from changing over time.

Solution: Perform a Subscription Health scan when packages are created.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead implement Continuous Assurance for the project.

Note: The Subscription Security health check features in AzSK contains a set of scripts that examines a subscription and flags off security issues, misconfigurations or obsolete artifacts/settings which can put your subscription at higher risk.

Reference:

<https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html>

NO.45 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 use Azure Pipelines to build and test a React js application.

You have a pipeline that has a single job.

You discover that installing JavaScript packages from npm takes approximately five minutes each time you run the pipeline.

You need to recommend a solution to reduce the pipeline execution time.

Solution: You recommend defining a container job that uses a custom container that has the

JavaScript packages preinstalled.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead enable pipeline caching.

Note:

npm-cache is a command line utility that caches dependencies installed via npm, bower, jspm and composer.

It is useful for build processes that run [npm|bower|composer|jspm] install every time as part of their build process. Since dependencies don't change often, this often means slower build times. npm-cache helps alleviate this problem by caching previously installed dependencies on the build machine.

Reference:

<https://www.npmjs.com/package/npm-cache>

NO.46 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: A

Explanation

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

NO.47 Your company develops an application named App1 that is deployed in production.

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

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

What should you do?

A. Create a branch in the build.

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

Answer: D

Reference:

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

NO.48 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

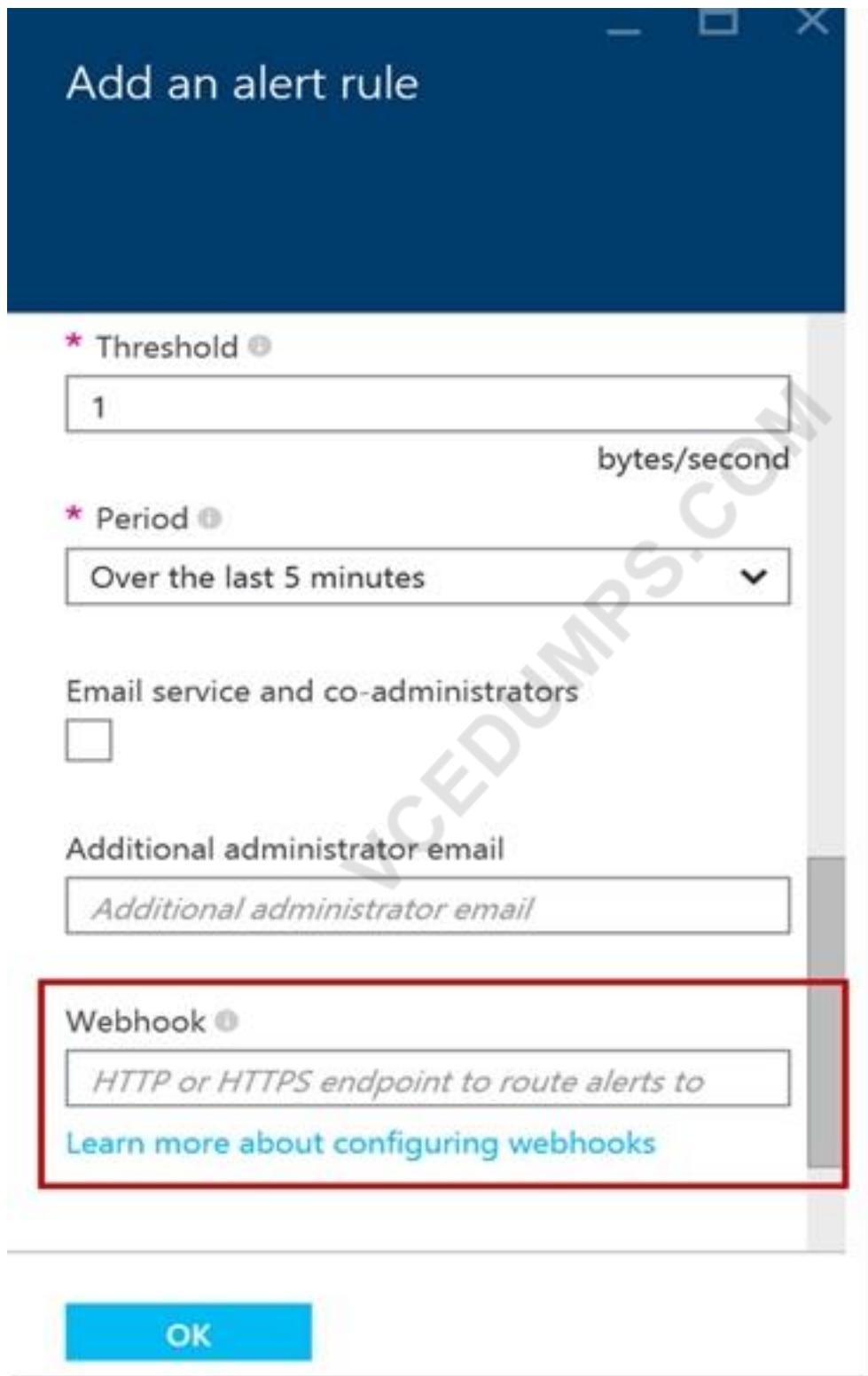
Resource Group: az400-9940427-main

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/>

NO.49 You are defining release strategies for two applications as shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

Release Strategies

Blue/Green deployment

Canary deployment

Rolling deployment

Answer Area:

App1:

App2:

Answer:

Release Strategies

Blue/Green deployment

Canary deployment

Rolling deployment

Answer Area:

App1:

Canary deployment

App2:

Rolling deployment

Explanation

App1: **Canary deployment**

App2: **Rolling deployment**

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.

NO.50 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

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>

NO.51 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.

Branch lifetime:

Long-lived	
Short-lived	

Branch type:

Master	
Feature	
Integration	

Answer:

Branch lifetime:

	▼
Long-lived	
Short-lived	

Branch type:

	▼
Master	
Feature	
Integration	

Explanation

Branch lifetime:

	▼
Long-lived	
Short-lived	

Branch type:

	▼
Master	
Feature	
Integration	

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>

NO.52 You are designing a configuration management solution to support five apps hosted on Azure App Service.

Each app is available in the following three environments: development, test, and production.

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

requirements:

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

A. Azure Cosmos DB

B. Azure App Service

C. Azure App Configuration

D. Azure Key Vault

Answer: C

Explanation

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

App Configuration offers the following benefits:

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

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

Reference:

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

NO.53 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.

Global release:

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

Production stage:

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

Answer:

Actions

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



Answer Area

- 1 Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1.
- 2 Run the Import-AzureRmAutomationDscConfiguration Azure PowerShell cmdlet.
- 3 Run the Start-AzureRmAutomationDscCompilationJob Azure PowerShell cmdlet.



Explanation

Global release:

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

Production stage:

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

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>

NO.54 You plan to store signed images in an Azure Container Registry instance named az4009940427acr1.

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

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

Answer:

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.

The screenshot shows the 'myregistry - Content Trust' page in the Azure portal. On the left, there's a sidebar with 'Services' (Repositories, Webhooks, Replications, Tasks) and 'Policies' (Content trust, which is selected and highlighted with a red border). At the top right are 'Save' and 'Discard' buttons. A note says: 'When turned on, content trust enables you to push trusted images to the registry.' Below it, the 'Status' is shown as 'Enabled'.

References:

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

NO.55 You need to configure access to Azure DevOps Agent pools to meet the forwarding requirements:

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

Which role memberships are required for the Azure DevOps organization and the project? To answer, drag the appropriate role membership to the correct targets. Each role membership may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to content NOTE: Each correct selection is worth one point.

Roles

Answer Area

Administrator

Organization:

Reader

Project:

Service Account

User

Answer:

Roles**Answer Area**

- Administrator
- Reader
- Service Account
- User

Organization:

Reader

Project:

User

Explanation

project level role: User

Organization level role: Reader

References: <https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues>**NO.56** You have an Azure web app named Webapp1.

You need to use an Azure Monitor query to create a report that details the top 10 pages of Webapp1 that failed.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

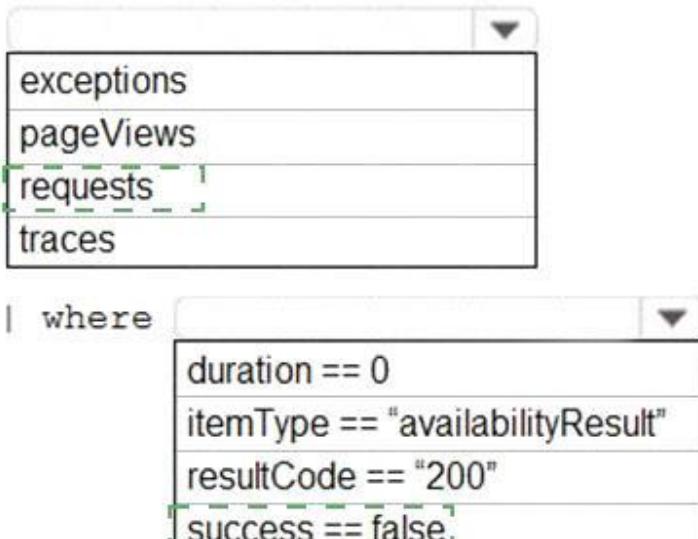
- | |
|------------|
| exceptions |
| pageViews |
| requests |
| traces |

| where

- | |
|----------------------------------|
| duration == 0 |
| itemType == "availabilityResult" |
| resultCode == "200" |
| success == false |

```
| summarize failedCount=sum(itemCount) by name, resultCode
| top 10 by failedCount desc
| render barchart
```

Answer:



```

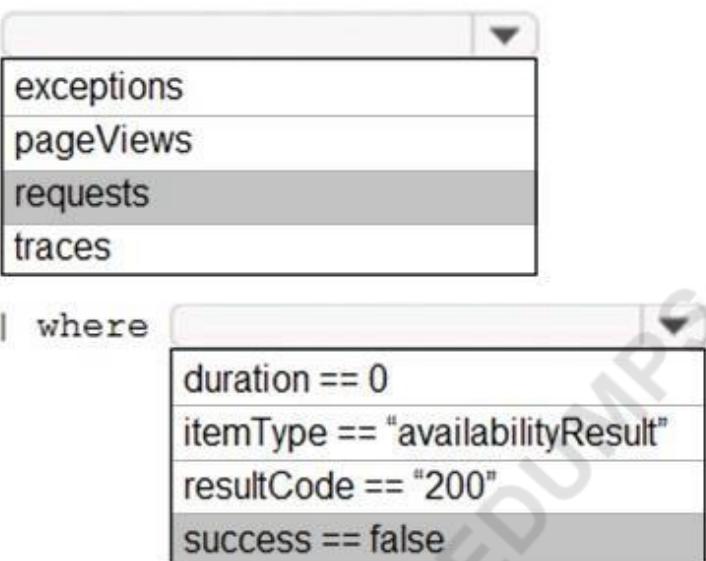
exceptions
pageViews
requests
traces

| where
    duration == 0
    itemType == "availabilityResult"
    resultCode == "200"
    success == false

| summarize failedCount=sum(itemCount) by name, resultCode
| top 10 by failedCount desc
| render barchart

```

Explanation



```

exceptions
pageViews
requests
traces

| where
    duration == 0
    itemType == "availabilityResult"
    resultCode == "200"
    success == false

| summarize failedCount=sum(itemCount) by name, resultCode
| top 10 by failedCount desc
| render barchart

```

Box 1: requests

Failed requests (requests/failed):

The count of tracked server requests that were marked as failed.

Kusto code:

requests

| where success == 'False'

Box 2: success == false

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/app-insights-metrics>

NO.57 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.** npmj.org
- C.** Maven Central
- D.** third-party trusted Python

Answer: A

Explanation

Get started with Python packages in Azure Artifacts

Create a feed

* Select Artifacts (in the left navigation of your Azure DevOps project).

* On the Artifacts page, select Create Feed.

* In the Create new feed dialog box:

* In the Name field, give the feed a name.

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

Reference:

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

NO.58 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure DevOps project.

Your build process creates several artifacts.

You need to deploy the artifacts to on-premises servers.

Solution: You deploy a Kubernetes cluster on-premises. You deploy a Helm agent to the cluster. You add a Download Build Artifacts task to the deployment pipeline.

Does this meet the goal?

- A.** Yes
- B.** No

Answer: B

Explanation

Instead you should deploy an Azure self-hosted agent to an on-premises server.

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

Note 2: As we [Microsoft] are launching this new experience in preview, we are currently optimizing it for Azure Kubernetes Service (AKS) and Azure Container Registry (ACR). Other Kubernetes clusters, for example running on-premises or in other clouds, as well as other container registries, can be used, but require setting up a Service Account and connection manually.

References:

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

NO.59 Your company has a project in Azure DevOps.

You need to ensure that when there are multiple builds pending deployment only the most recent build is deployed.

What should you use?

- A.** deployment queue settings
- B.** deployment conditions
- C.** release gates
- D.** pull request triggers

Answer: A

Explanation

References:

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

NO.60 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure DevOps project.

Your build process creates several artifacts.

You need to deploy the artifacts to on-premises servers.

Solution: You deploy an Octopus Deploy server. You deploy a polled Tentacle agent to an on-premises server.

You add an Octopus task to the deployment pipeline.

Does this meet the goal?

- A.** Yes

- B.** No

Answer: B

Explanation

Instead you should deploy an Azure self-hosted agent to an on-premises server.

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

Reference:

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

NO.61 You have a project in Azure DevOps. You have an Azure Resource Group deployment project in Microsoft Visual Studio that is checked in to the Azure DevOps project.

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

The solution must minimize administrative effort.

Which task type should you include in the solution?

- A.** Azure Cloud Service Deployment
- B.** Azure RM Web App Deployment
- C.** Azure PowerShell
- D.** Azure App Service Manage

Answer: C

Explanation

There are two different ways to deploy templates to Azure DevOps Services. Both methods provide the same results, so choose the one that best fits your workflow.

1. Add a single step to your build pipeline that runs the PowerShell script that's included in the Azure Resource Group deployment project (Deploy-AzureResourceGroup.ps1). The script copies artifacts and then deploys the template.

2. Add multiple Azure DevOps Services build steps, each one performing a stage task.

The first option has the advantage of using the same script used by developers in Visual Studio and providing consistency throughout the lifecycle.

References:

<https://docs.microsoft.com/en-us/azure/vs-azure-tools-resource-groups-ci-in-vsts>

NO.62 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:

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

Deployment 2:

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

Deployment 3:

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

Explanation

Deployment 1:

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

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.

NO.63 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage a project in Azure DevOps.

You need to prevent the configuration of the project from changing over time.

Solution: Implement Continuous Assurance for the project.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation

The basic idea behind Continuous Assurance (CA) is to setup the ability to check for "drift" from what is considered a secure snapshot of a system. Support for Continuous Assurance lets us treat security truly as a

'state' as opposed to a 'point in time' achievement. This is particularly important in today's context when

'continuous change' has become a norm.

There can be two types of drift:

- * Drift involving 'baseline' configuration: This involves settings that have a fixed number of possible states (often pre-defined/statically determined ones). For instance, a SQL DB can have TDE encryption turned ON or OFF...or a Storage Account may have auditing turned ON however the log retention period may be less than 365 days.

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

Reference:

<https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html>

NO.64 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure DevOps project.

Your build process creates several artifacts.

You need to deploy the artifacts to on-premises servers.

Solution: You deploy a Docker build to an on-premises server. You add a Download Build Artifacts task to the deployment pipeline.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead you should deploy an Azure self-hosted agent to an on-premises server.

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

References:

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

NO.65 You have a project in Azure DevOps that has three teams as shown in the Teams exhibit.
(Click the Teams tab.)

The screenshot shows the 'Project Settings' page for the 'Contoso' team. In the left sidebar, under 'General', the 'Dashboards' option is selected. On the right, the 'Dashboards' section displays the following permissions for the team:

- Create dashboards
- Edit dashboards
- Delete dashboards

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.)

This screenshot is identical to the one above, showing the 'Project Settings' page for the 'Contoso' team. The 'Dashboards' section displays the same set of permissions:

- Create dashboards
- Edit dashboards
- Delete dashboards

All other permissions have the default values set.

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

Answer:

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

Explanation

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

NO.66 You have an Azure DevOps project that uses many package feeds.

You need to simplify the project by using a single feed that stores packages produced by your company and packages consumed from remote feeds. The solution must support public feeds and authenticated feeds.

What should you enable in DevOps?

- A. Universal Packages
- B. views in Azure Artifacts
- C. upstream sources
- D. a symbol server

Answer: B

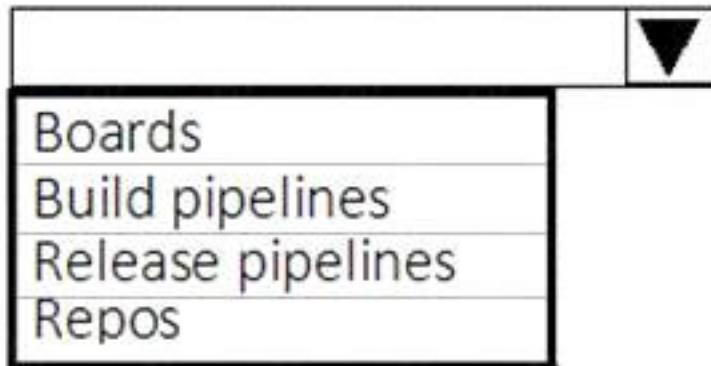
NO.67 You currently use JIRA, Jenkins, and Octopus as part of your DevOps processes.

You plan to use Azure DevOps to replace these tools.

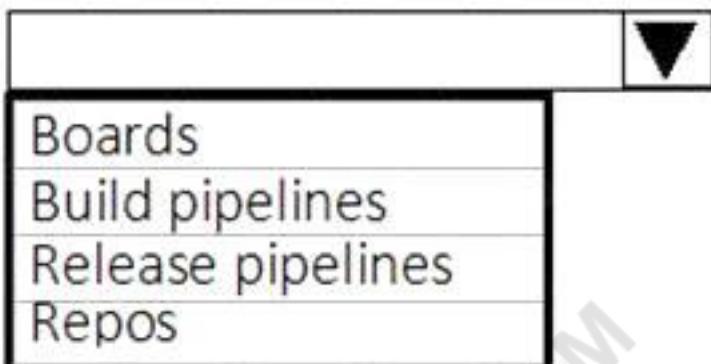
Which Azure DevOps service should you use to replace each tool? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

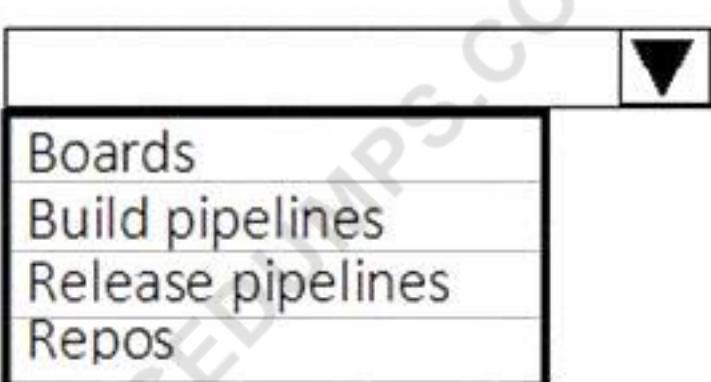
JIRA:



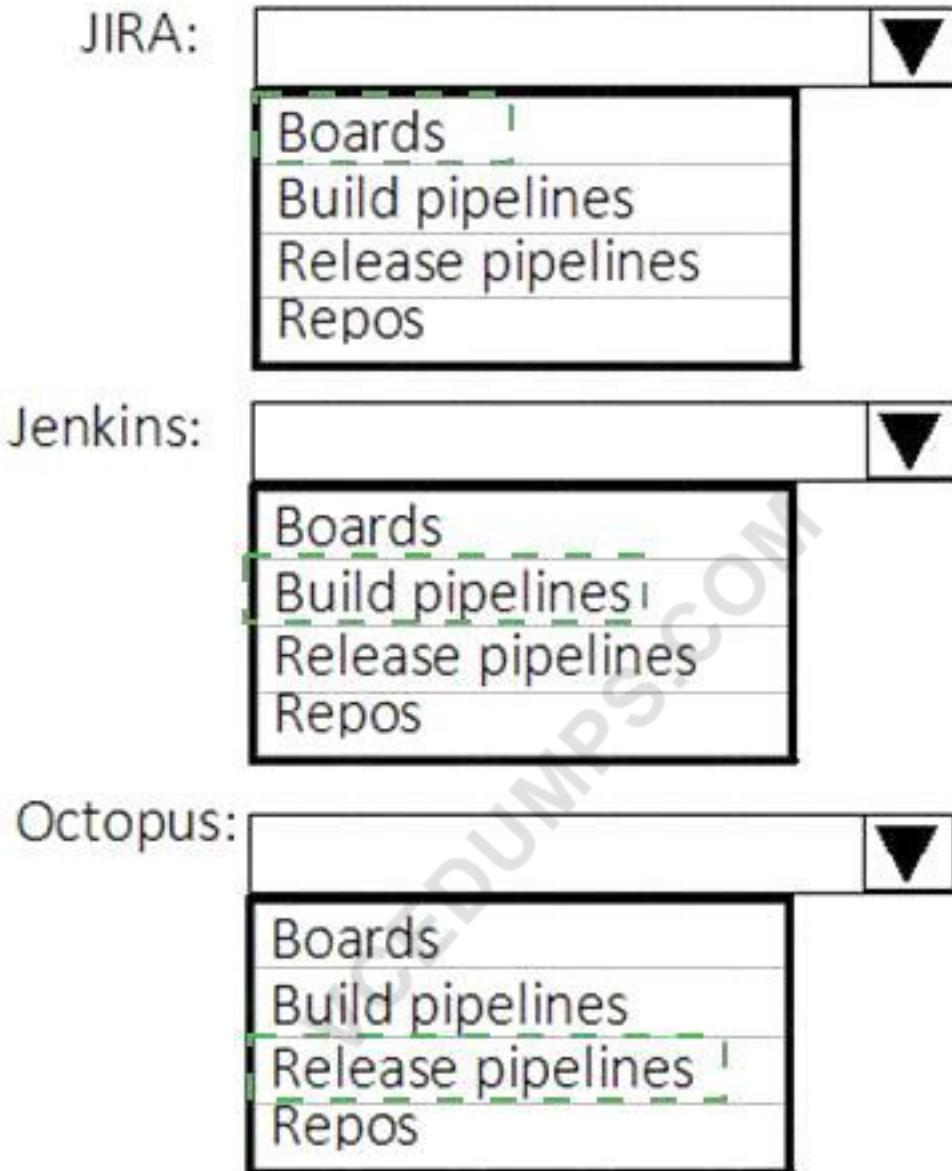
Jenkins:



Octopus:



Answer:



Explanation

JIRA- Board Jenkins- Build Pipelines

NO.68 Your company builds a multi tier web application.

> You use Azure DevOps and host the production application on Azure virtual machines.

Your team prepares an Azure Resource Manager template of the virtual machine that you will use to test new features.

You need to create a staging environment in Azure that meets the following requirements:

- * Minimizes the cost of Azure hosting
- * Provisions the virtual machines automatically
- * Use* the custom Azure Resource Manager template to provision the virtual machines What should you do?

A. In Azure DevOps, configure new tasks in the release pipeline to create and delete the virtual machines in Azure DevTest Labs.

B. From Azure Cloud Shell, run Azure PowerShell commands to create and delete the new virtual machines in a staging resource group.

- C.** In Azure DevOps, configure new tasks in the release pipeline to deploy to Azure Cloud Services.
D. In Azure Cloud Shell, run Azure CLI commands to create and delete the new virtual machines in a staging resource group.

Answer: A

Explanation

You can use the Azure DevTest Labs Tasks extension that's installed in Azure DevOps to easily integrate your CI/CD build-and-release pipeline with Azure DevTest Labs. The extension installs three tasks:

- * Create a VM
- * Create a custom image from a VM
- * Delete a VM

The process makes it easy to, for example, quickly deploy a "golden image" for a specific test task and then delete it when the test is finished.

References: <https://docs.microsoft.com/en-us/azure/lab-services/devtest-lab-integrate-ci-cd-vsts>

NO.69 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.

Containers must only be published internally:

Azure Container Instances
Azure Container Registry
Dockerfile

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

An Azure Active Directory (Azure AD) group
An Azure Automation account
An Azure service principal

Answer:

Containers must only be published internally:

Azure Container Instances
Azure Container Registry
Dockerfile

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

An Azure Active Directory (Azure AD) group
An Azure Automation account
An Azure service principal

Explanation

Containers must only be published internally:

Azure Container Instances
Azure Container Registry
Dockerfile

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

An Azure Active Directory (Azure AD) group
An Azure Automation account
An Azure service principal

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>

NO.70 You are finalizing a release in GitHub.

You need to apply the following labels to the release:

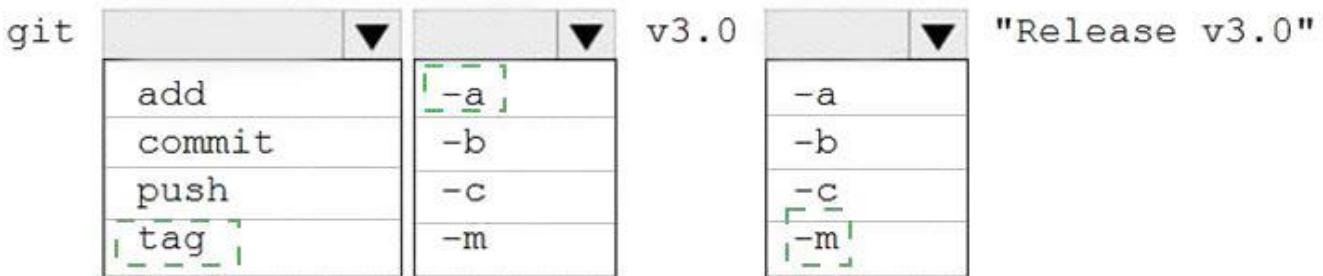
- * Name
- * Email
- * Release v3.0
- * Release date

How should you complete the git command? To answer, select the appropriate options in the answer area.

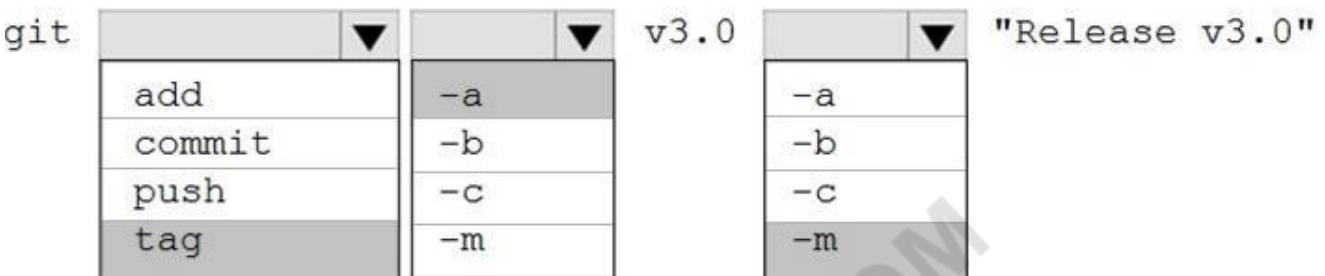
NOTE: Each correct selection is worth one point.

git	▼	▼	v3.0	▼	"Release v3.0"
add		-a	-a		
commit		-b	-b		
push		-c	-c		
tag		-m	-m		

Answer:



Explanation



Box 1: tag

Tagging. Like most VCSs, Git has the ability to tag specific points in a repository's history as being important.

Typically, people use this functionality to mark release points (v1.0, v2.0 and so on).

Box 2: -a

Creating an annotated tag in Git is simple. The easiest way is to specify -a when you run the tag command:

Example:

```
$ git tag -a v1.4 -m "my version 1.4"
```

Box 3: -m

Reference:

<https://git-scm.com/book/en/v2/Git-Basics-Tagging>

NO.71 Your company has a project in Azure DevOps.

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

The templates will reference secrets stored in Azure Key Vault.

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

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

NOTE: Each correct selection is worth one point.

Configurations

Answer Area

A Key Vault access policy

Enable key vaults for template deployment by using:

A Key Vault advanced access policy

Restrict access to the secrets in Key Vault by using:

RBAC

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

A Key Vault access policy

Enable key vaults for template deployment by using: A Key Vault advanced access policy

A Key Vault advanced access policy

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

RBAC

Explanation**Answer Area**

Enable key vaults for template deployment by using: A Key Vault advanced access policy

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

Box 1: A key Vault advanced access policy

Home > mykeyvaulttutorialrg > mykeyvault0920 - Access policies

mykeyvault0920 - Access policies

Key vault

Save Discard Refresh

Click to hide advanced access policies

Enable access to Azure Virtual Machines for deployment

Enable access to Azure Resource Manager for template deployment

Enable access to Azure Disk Encryption for volume encryption

Add new

<Your username> USER

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Keys
- Secrets
- Certificates
- Access policies
- Firewalls and virtual networks

Box 2: RBAC

Management plane access control uses RBAC.

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

- * Creating or deleting a key vault.
- * Getting a list of vaults in a subscription.
- * Retrieving Key Vault properties (such as SKU and tags).

* Setting Key Vault access policies that control user and application access to keys and secrets.

References:

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

NO.72 You are automating the testing process for your company.

You need to automate UI testing of a web application.

Which framework should you use?

- A.** JaCoco
- B.** Selenium
- C.** Xamarin.UITest
- D.** Microsoft.CodeAnalysis

Answer: B

Explanation

Performing user interface (UI) testing as part of the release pipeline is a great way of detecting unexpected changes, and need not be difficult. Selenium can be used to test your website during a continuous deployment release and test automation.

References:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/test/continuous-test-selenium?view=azure-devops>

NO.73 You have an Azure DevOps project named Project1 and an Azure subscription named Sub1. Sub1 contains an Azure virtual machine scale set named VMSS1. VMSS1 hosts a web application named WebApp1.

WebApp1 uses stateful sessions.

The WebApp1 installation is managed by using the Custom Script extension. The script resides in an Azure Storage account named sa1.

You plan to make a minor change to a UI element of WebApp1 and to gather user feedback about the change.

You need to implement limited user testing for the new version of WebApp1 on VMSS1.

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

NOTE: Each correct selection is worth one point.

- A.** Modify the load balancer settings of VMSS1.
- B.** Redeploy VMSS1.
- C.** Upload a custom script file to sa1.
- D.** Modify the Custom Script extension settings of VMSS1.
- E.** Update the configuration of a virtual machine in VMSS1.

Answer: B C D

NO.74 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

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

You use a Git repository for applications source control.

You need to implement a pull request strategy that reduces the history volume in the master branch.

Solution: You implement a pull request strategy that uses squash merges.

Does this meet the goal?

A. Yes

B. No

Answer: A

NO.75 Note: This question part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

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

Solution: You add a trigger to the build pipeline.

Does this meet the goal?

A. Yes

B. NO

Answer: B

Explanation

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

References:

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

NO.76 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You need to ensure that when code is checked in, a build runs automatically.

Solution: From the Pre-deployment conditions settings of the release pipeline, you select After stage.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

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

* Select the Triggers tab.

* Enable Continuous integration.

References:

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

NO.77 Your company has an on-premises Bitbucket Server that is used for Git-based source control.

The server is protected by a firewall that blocks inbound Internet traffic.

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

Which two components are required to integrate Azure DevOps and Bitbucket?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: A D

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>

NO.78 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your company has a project in Azure DevOps for a new web application.

You need to ensure that when code is checked in, a build runs automatically.

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

Does this meet the goal?

- A.** Yes

- B.** No

Answer: B

Explanation

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

- * Select the Triggers tab.
- * Enable Continuous integration.

References:

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

NO.79 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

Answer: C E

Explanation

<https://docs.microsoft.com/en-us/azure/security-center/features-paas>

NO.80 Your company plans to implement a new compliance strategy that will require all Azure web apps to be backed up every five hours.

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

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

Answer:

See solution below.

Explanation

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

* Open the App Service az400-11566895-main, which you want to protect, in the Azure Portal and browse to Settings > Backups. Click Configure and a Backup Configuration blade should appear.

* Select the storage account.

* Click + to create a private container. You could name this container after the web app or App Service.

* Select the container.

* If you want to schedule backups, then set Scheduled Backup to On and configure a schedule: every five hours

* Select your retention. Note that 0 means never delete backups.

* Decide if at least one backup should always be retained.

* Choose if any connected databases should be included in the web app backup.

* Click Save to finalize the backup configuration.

The screenshot shows the 'Backup Configuration' window with three main sections:

- Backup Storage**: Selects the target container for app backups, with a storage account named 'petriaspbackup.blob.core.windows.net'.
- Backup Schedule**: Configures a scheduled backup. It's set to 'On', 'Backup Every 1 Days', and starts at '2018-01-20 16:31:38 UTC'. The retention period is set to 3655 days.
- Backup Database**: Selects databases for backup. A single database, 'Included', is selected with a connection string 'defaultConnection' and type 'Sql Database'.

Reference:

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

NO.81 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

Explanation

References:

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

NO.82 You have a containerized solution that runs in Azure Container Instances. The solution contains a frontend container named App1 and a backend container named DB1. DB1 loads a large amount of data during startup.

You need to verify that DB1 can handle incoming requests before users can submit requests to Appl. What should you configure?

A. a liveness probe

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

Answer: C

Explanation

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

Reference:

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

NO.83 You have an existing build pipeline in Azure Pipelines.

You need to use incremental builds without purging the environment between pipeline executions.

What should you use?

- A. a File Transform task
- B. a self-hosted agent
- C. Microsoft-hosted parallel jobs

Answer: B

Explanation

When you run a pipeline on a self-hosted agent, by default, none of the subdirectories are cleaned in between two consecutive runs. As a result, you can do incremental builds and deployments, provided that tasks are implemented to make use of that. You can override this behavior using the workspace setting on the job.

Reference:

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

NO.84 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 company has a prefect in Azure DevOps for a new web application.

You need to ensure that when code is checked in, a build runs automatically.

Solution: From the Triggers tab of the build pipeline, you selected Batch changes while a build is in progress Does this meet the goal?

A. Yes

B. No

Answer: B

NO.85 You have an Azure DevOps project named Project1 and an Azure subscription named Sub1. Sub1 contains an Azure SQL database named DB1.

You need to create a release pipeline that uses the Azure SQL Database Deployment task to update DB1.

Which artifact should you deploy?

- A. a BACPAC

- B.** a DACPAC
- C.** an LDF file
- D.** an MDF file

Answer: B

Explanation

Use Azure SQL Database Deployment task in a build or release pipeline to deploy to Azure SQL DB using a DACPAC or run scripts using SQLCMD.

Reference:

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

NO.86 You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant. You are configuring a build pipeline in Azure Pipelines that will include a task named Task1. Task1 will authenticate by using an Azure AD service principal.

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

NOTE: Each correct selection is worth one point.

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

Answer: B C D

Reference:

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

NO.87 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 use Azure Pipelines to build and test a React js application

You have a pipeline that has a single job.

You discover that installing JavaScript packages from npm takes approximately five minutes each time you run the pipeline.

You need to recommend a solution to reduce the pipeline execution time.

Solution: You recommend enabling pipeline caching.

Does this meet the goal?

- A.** Yes
- B.** No

Answer: A

Explanation

npm-cache is a command line utility that caches dependencies installed via npm, bower, jspm and composer.

It is useful for build processes that run [npm | bower | composer | jspm] install every time as part of their build process. Since dependencies don't change often, this often means slower build times. npm-cache helps alleviate this problem by caching previously installed dependencies on the build machine.

Reference:

<https://www.npmjs.com/package/npm-cache>

NO.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.

Chart Widgets Answer Area

Burndown

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

Cycle Time

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

Lead Time

The remaining work:

Answer:

Actions

Answer Area

Run the `Import-AzureRmAutomationDscConfiguration` Azure PowerShell cmdlet.

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

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

Run the `Import-AzureRmAutomationDscConfiguration` Azure PowerShell cmdlet.

Run the `New-AzureRmResourceGroupDeployment` Azure PowerShell cmdlet.



Run the `Start-AzureRmAutomationDscCompilationJob` Azure PowerShell cmdlet.



Run the `start-AzureRmAutomationDscCompilationJob` Azure PowerShell cmdlet.

Create an Azure Resource Manager template file that has an extension of .json.

Explanation

Answer Area

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

Lead Time

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

Cycle Time

The remaining work:

Burndown

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.

NO.89 Your team uses an agile development approach.

You need to recommend a branching strategy for the team's Git repository. The strategy must meet the following requirements.

Provide the ability to work on multiple independent tasks in parallel.

Ensure that checked-in code remains in a releasable state always.

Ensure that new features can be abandoned at any time.

Encourage experimentation.

What should you recommend?

- A. a single long-running branch
- B. multiple long-running branches
- C. a single fork per team member
- D. a single-running branch with multiple short-lived topic branches

Answer: D

Explanation

Topic branches, however, are useful in projects of any size. A topic branch is a short-lived branch that you create and use for a single particular feature or related work. This is something you've likely never done with a VCS before because it's generally too expensive to create and merge branches. But in Git it's common to create, work on, merge, and delete branches several times a day.

Reference:

<https://git-scm.com/book/en/v2/Git-Branching-Branching-Workflows>

NO.90 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

Explanation

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

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

Host your own agents on infrastructure that you manage.

Buy additional parallel jobs.

Reference:

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

NO.91 Your company is concerned that when developers introduce open source libraries, it creates licensing compliance issues.

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

What should you use?

- A.** SourceGear Vault
- B.** Jenkins
- C.** Microsoft Visual SourceSafe
- D.** WhiteSource Bolt

Answer: D

Explanation

WhiteSource provides WhiteSource Bolt, a lightweight open source security and management solution developed specifically for integration with Azure DevOps and Azure DevOps Server.

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

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

Reference:

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

NO.92 You plan to onboard 10 new developers.

You need to recommend a development environment that meets the following requirements:

- * Integrates with GitHub

- * Provides integrated debugging tools
- * Supports remote workers and hot-desking environments
- * Supports developers who use browsers, tablets, and Chromebooks

What should you recommend?

- A.** VS Code
- B.** Xamarin Studio
- C.** MonoDevelop
- D.** Visual Studio Codespaces

Answer: D

Explanation

Visual Studio Codespaces is built to accommodate the widest variety of projects or tasks, including GitHub and integrating debugging.

Visual Studio Codespaces conceptually and technically extends the Visual Studio Code Remote Development extensions.

In addition to "backend" environments, Visual Studio Codespaces supports these "frontend" editors:

- * Visual Studio Code
- * Visual Studio Code-based editor in the browser

Reference:

<https://docs.microsoft.com/sv-se/visualstudio/codespaces/overview/what-is-vsonline>

NO.93 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.** Continuous export
- C.** Smart Detection
- D.** custom events
- E.** usage analysis

Answer: C

Explanation

Smart Detection automatically warns you of potential performance problems and failure anomalies in your web application. It performs proactive analysis of the telemetry that your app sends to Application Insights. If there is a sudden rise in failure rates, or abnormal patterns in client or server performance, you get an alert.

Reference:

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

NO.94 You have an Azure subscription that contains resources in several resource groups.

You need to design a monitoring strategy that will provide a consolidated view. The solution must support the following requirements:

- * Support role-based access control (RBAC) by using Azure Active Directory (Azure AD) identities.
- * Include visuals from Azure Monitor that are generated by using the Kusto query language.
- * Support documentation written in markdown.

* Use the latest data available for each visual.

What should you use to create the consolidated view?

- A. Azure Data Explorer**
- B. Azure dashboards**
- C. Azure Monitor**
- D. Microsoft Power BI**

Answer: A

Explanation

There are several tools available for running queries in Azure Data Explorer, including Kusto.

Kusto uses a role-based access control (RBAC) model, under which authenticated principals are mapped to roles, and get access according to the roles they're assigned.

Note: Azure Data Explorer is a highly scalable and secure analytics service that enables you to do rich exploration of structured and unstructured data for instant insights. Optimized for ad-hoc queries, Azure Data Explorer enables rich data exploration over raw, structured, and semi-structured data delivering fast time to insight. Query with a modern, intuitive query language that offers fast, ad-hoc, and advanced query capabilities over high-rate data volumes and varieties Reference:

<https://docs.microsoft.com/en-us/azure/data-explorer/tools-integrations-overview>

NO.95 Your company implements an Agile development methodology.

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

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

NOTE: Each correct selection is worth one point.

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

Answer: C D E

Explanation

<https://www.scrum.org/resources/what-is-a-sprint-retrospective>

NO.96 Your company uses Service Now for incident management.

You develop an application that runs on Azure.

The company needs to generate a ticket in Service Now when the application fails to authenticate.

Which Azure Log Analytics solution should you use?

- A. Automation & Control**
- B. IT Service Management Connector (ITSM)**
- C. Application ImiQ.hu Connector**
- D. insight & Analytics**

Answer: B

Explanation

The IT Service Management Connector (ITSMC) allows you to connect Azure and a supported IT Service Management (ITSM) product/service.

ITSMC supports connections with the following ITSM tools:

- * ServiceNow
- * System Center Service Manager
- * Provance
- * Cherwell

With ITSMC, you can

- * Create work items in ITSM tool, based on your Azure alerts (metric alerts, Activity Log alerts and Log Analytics alerts).
- * Optionally, you can sync your incident and change request data from your ITSM tool to an Azure Log Analytics workspace.

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

NO.97 You are configuring the settings of a new Git repository in Azure Repos.

You need to ensure that pull requests in a branch meet the following criteria before they are merged:

- * Committed code must compile successfully.
- * Pull requests must have a Quality Gate status of Passed in SonarCloud.

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

NOTE: Each correct selection is worth one point.

Policy Types

A build policy

A check-in policy

A status policy

Committed code must compile successfully:

Pull requests must have a Quality Gate status of Passed in SonarCloud:

Answer:

Policy Types

A build policy

A check-in policy

A status policy

Committed code must compile successfully:

A check-in policy

Pull requests must have a Quality Gate status of Passed in SonarCloud:

A build policy

Explanation

Committed code must compile successfully:

A check-in policy

Pull requests must have a Quality Gate status of Passed in SonarCloud:

A build policy

Box 1: A check-in policy

Administrators of Team Foundation version control can add check-in policy requirements. These check-in policies require the user to take actions when they conduct a check-in to source control.

By default, the following check-in policy types are available:

- * Builds Requires that the last build was successful before a check-in.
- * Code Analysis Requires that code analysis is run before check-in.
- * Work Items Requires that one or more work items be associated with the check-in.

Box 2: Build policy

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/add-check-policies>

<https://azuredavolabs.com/labs/vstsextend/sonarcloud/>

NO.98 Your company uses Azure DevOps to manage the build and release processes for applications.

You use a Git repository for applications source control.

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

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

Which pull request action should you use?

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

Answer: C

Explanation

Cherry-pick a pull request

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

* In a completed pull request, select Cherry-pick, or for an active pull request, select Cherry-pick from the

... menu. Cherry-picking a pull request in this way creates a new branch with the copied changes.

Merge into a target branch in a second pull request.

* In Target branch, enter the branch you want to merge the copied changes.

* In Topic branch name, enter a new branch to contain the copied changes, then select Cherry-pick.

* Select Create pull request to merge the topic branch into the target branch to complete the cherry-pick.

Reference:

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

NO.99 Your company is building a mobile app that targets Android devices and iOS devices. Your team uses Azure DevOps to manage all work items and release cycles. You need to recommend a solution to perform the following tasks:

- * Collect crash reports for issue analysis
- * Distribute beta releases to your testers.
- * Get user feedback on the functionality of new apps.

What should you include in the recommendation?

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

Answer: C

Explanation

The "Exploratory Testing" extension is now "Test & Feedback" and is now Generally Available. Anyone can now test web apps and give feedback, all directly from the browser on any platform: Windows, Mac, or Linux. Available for Google Chrome and Mozilla Firefox (required version 50.0 or above) currently.

Support for Microsoft Edge is in the pipeline and will be enabled once Edge moves to a Chromium-compatible web platform.

References:

<https://marketplace.visualstudio.com/items?itemName=ms.vss-exploratorytesting-web>

NO.100 You have a web app hosted on Azure App Service. The web app stores data in an Azure SQL database.

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

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

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

Answer: A

Explanation

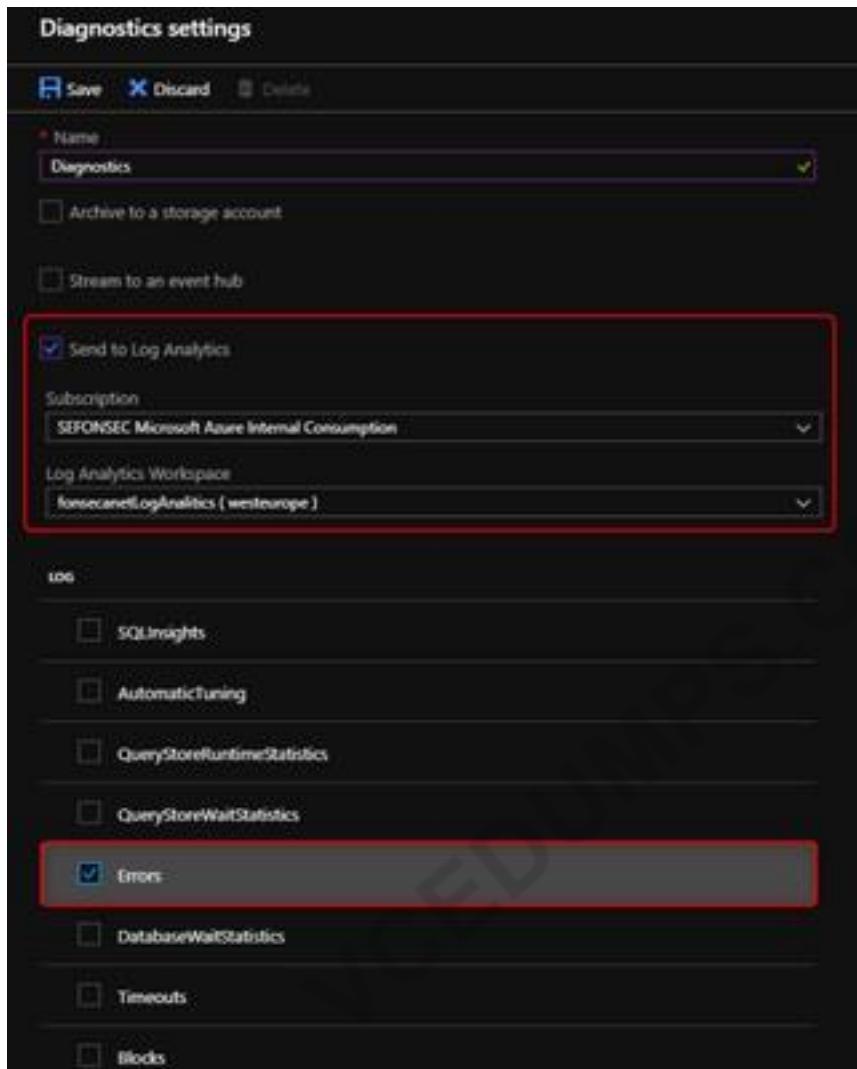
ENABLE DIAGNOSTICS TO LOG ANALYTICS

This configuration is done PER DATABASE

1. Click on Diagnostics Settings and then Turn On Diagnostics

The screenshot shows the Azure portal interface for managing diagnostic settings for the AdventureWorks database. The left sidebar contains navigation links for Connection strings, Sync to other databases, Add Azure Search, Properties, Locks, Export template, Security (Advanced Data Security, Auditing, Dynamic Data Masking, Transparent data encryption), Intelligent Performance (Performance overview, Performance recommendations, Query Performance Insight, Automatic tuning), Monitoring (Alerts (Classic), Metrics, Diagnostic settings), and Support + troubleshooting. The 'Diagnostic settings' link is highlighted with a red box. The main content area displays the 'AdventureWorks (fonsecanet/AdventureWorks) - Diagnostic settings' page. It includes a 'Subscription' dropdown set to 'SEFONSEC Microsoft Azure Internal Consumption', a 'Resource group' dropdown set to 'CSSAzureDB', and a 'Log Analytics workspace' dropdown set to 'LogAnalytics'. A large red box highlights the 'Send to Log Analytics' section, which lists the following data types to collect: SQLInsights, AutomaticTuning, QueryStoreRuntimeStatistics, QueryStoreWaitStatistics, Errors, DatabaseWaitStatistics, Timeouts, Blocks, Deadlocks, Audit, SQLSecurityAuditEvents, and AllMetrics.

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



Reference:

<https://techcommunity.microsoft.com/t5/azure-database-support-blog/azure-sql-db-and-log-analytics-better-together/ba-p/1000000000000000000>

NO.101 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company uses Azure DevOps to manage the build and release processes for applications. You use a Git repository for applications source control.

You need to implement a pull request strategy that reduces the history volume in the master branch.

Solution: You implement a pull request strategy that uses an explicit merge.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead use fast-forward merge.

Note:

No fast-forward merge - This option merges the commit history of the source branch when the pull request closes and creates a merge commit in the target branch.

Reference:

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

NO.102 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 Appl and deploy Appl to VMSS1. Appl 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 Appl. The solution must minimize administrative effort.

What should you include in the recommendation?

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

Answer: C

Explanation

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

Reference:

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

NO.103 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.** Create and run an Azure Container Registry task.
- B.** Add a Docker Hub service connection to Azure Pipelines.
- C.** Enable the Azure Event Grid resource provider and subscribe to registry events.
- D.** Create a service hook in Project1.

Answer: A

Explanation

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

Reference:

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

NO.104 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

D18912E1457D5D1DDCBD40AB3BF70D5D

Answer: B

Explanation

The Azure Artifacts Credential Provider automates the acquisition of credentials needed to restore NuGet packages as part of your .NET development workflow. It integrates with MSBuild, dotnet, and NuGet(.exe) and works on Windows, Mac, and Linux. Any time you want to use packages from an Azure Artifacts feed, the Credential Provider will automatically acquire and securely store a token on behalf of the NuGet client you're using.

Reference:

<https://github.com/Microsoft/artifacts-credprovider>

NO.105 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

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>

NO.106 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

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>

NO.107 You are configuring Azure Pipelines for three projects in Azure DevOps as shown in the following table.

Project name	Project Details
Project1	The project team provides preconfigured YAML files that it wants to use to manage future pipeline configuration changes.
Project2	The sensitivity of the project requires that the source code be hosted on the managed Windows server on your company's network.
Project3	The project team requires a centralized version control system to ensure that developers work with the most recent version.

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

NOTE: Each correct selection is worth one point.

Version Control Systems

Assembla Subversion

Bitbucket Cloud

Git in Azure Repos

GitHub Enterprise

Answer Area

Project1:

Project2:

Project3:

Answer:**Version Control Systems**

Assembla Subversion

Bitbucket Cloud

Git in Azure Repos

GitHub Enterprise

Answer Area

Project1:

 Git in Azure Repos

Project2:

 GitHub Enterprise

Project3:

 Bitbucket Cloud
 Explanation

Project1: Git in Azure Repos

Project2: GitHub Enterprise

Project3: Bitbucket Cloud

Project1: Git in Azure Repos

Project2: GitHub Enterprise

GitHub Enterprise is the on-premises version of GitHub.com. GitHub Enterprise includes the same great set of features as GitHub.com but packaged for running on your organization's local network. All repository data is stored on machines that you control, and access is integrated with your organization's authentication system (LDAP, SAML, or CAS).

Project3: Bitbucket cloud

One downside, however, is that Bitbucket does not include support for SVN but this can be easily amended migrating the SVN repos to Git with tools such as SVN Mirror for Bitbucket.

Note: SVN is a centralized version control system.

NO.108 You need to configure a cloud service to store the secrets required by the mobile applications to call the share.

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

Each correct selection is worth one point.

Required secrets:

Certificate
Personal access token
Shared Access Authorization token
Username and password

Storage location:

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

Answer:

Required secrets:

Certificate
Personal access token
Shared Access Authorization token
Username and password

Storage location:

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

Explanation

Required secrets:

Certificate
Personal access token
Shared Access Authorization token
Username and password

Storage location:

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

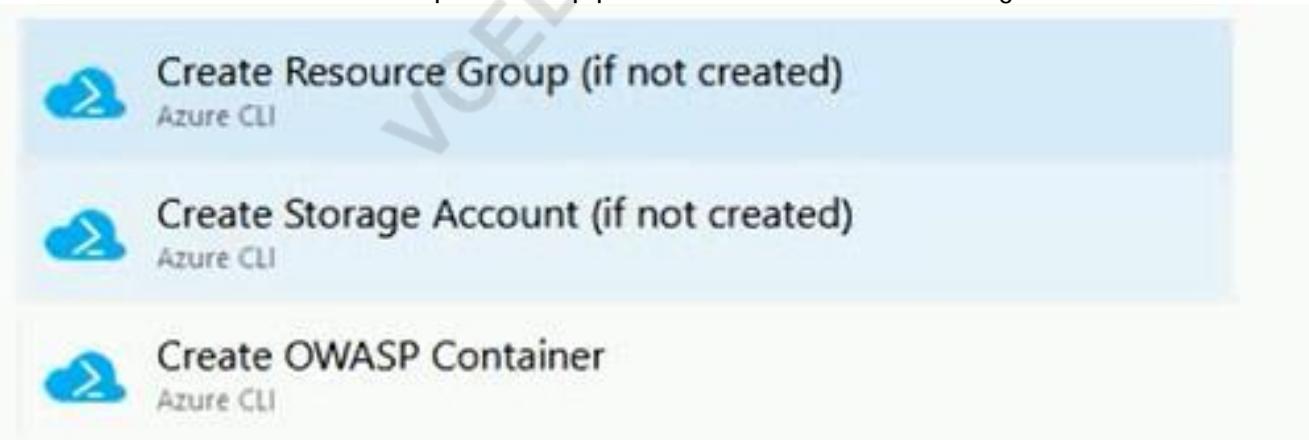
Every request made against a storage service must be authorized, unless the request is for a blob or container resource that has been made available for public or signed access. One option for authorizing a request is by using Shared Key.

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.

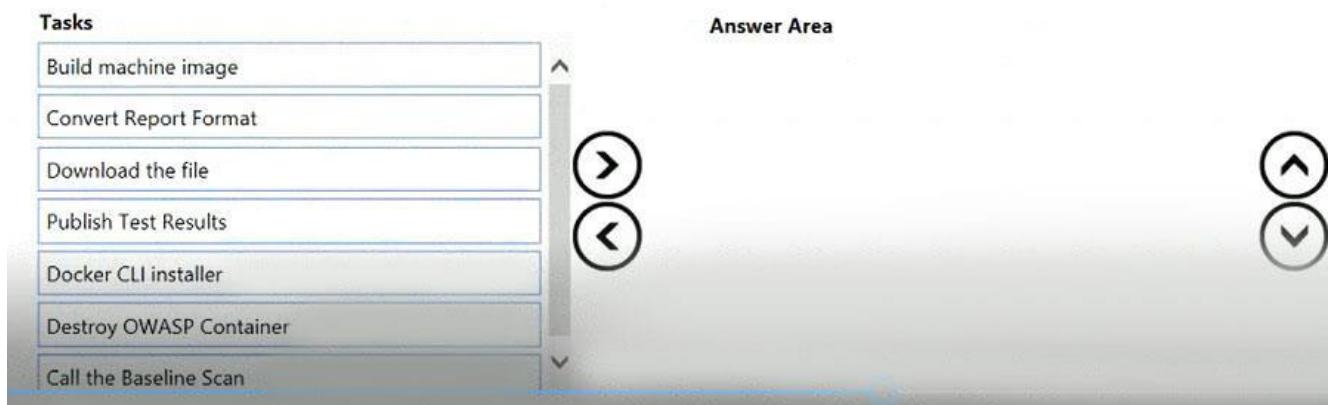
References: <https://docs.microsoft.com/en-us/rest/api/storageservices/authorize-with-shared-key>

NO.109 You have an Azure DevOps release pipeline as shown in the following exhibit.

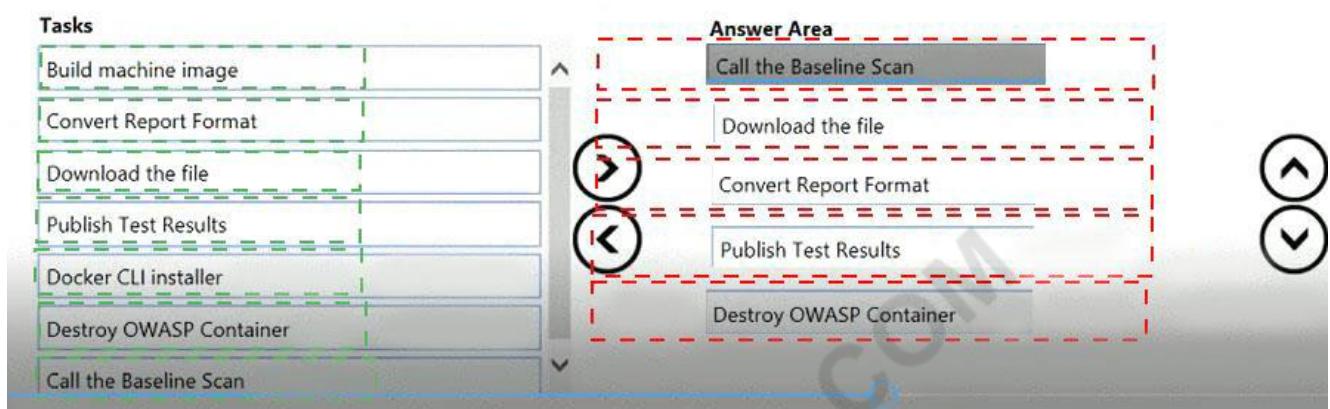


You need to complete the pipeline to configure OWASP ZAP for security testing.

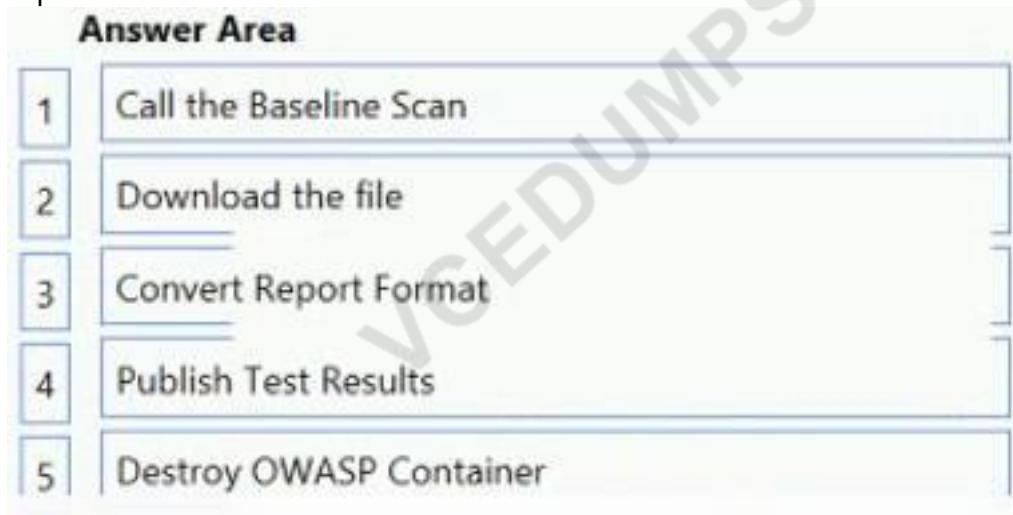
Which five Azure CLI tasks should you add in sequence? To answer, move the tasks from the list of tasks to the answer area and arrange them in the correct order.



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.

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

Reference:

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

NO.110 You have an application that consists of several Azure App Service web apps and Azure functions.

You need to access the security of the web apps and the functions.

Which Azure features can you use to provide a recommendation for the security of the application?

- A. Security & Compliance in Azure Log Analytics
- B. Resource health in Azure Service Health
- C. Smart Detection in Azure Application Insights
- D. Compute & apps in Azure Security Center

Answer: D

Explanation

Monitor compute and app services: Compute & apps include the App Services tab, which App services: list of your App service environments and current security state of each.

Recommendations

This section has a set of recommendations for each VM and computer, web and worker roles, Azure App Service Web Apps, and Azure App Service Environment that Security Center monitors. The first column lists the recommendation. The second column shows the total number of resources that are affected by that recommendation. The third column shows the severity of the issue.

NO.111 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

Two resource groups

Four Azure virtual machines in one resource group

Two Azure SQL databases in other resource group

You need to recommend a solution to deploy the resources.

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

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Use two templates, one for each resource group, and link the templates.

References:

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

NO.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 plan to update the Azure DevOps strategy of your company.

You need to identify the following issues as they occur during the company's development process:

* Licensing violations

* Prohibited libraries

Solution: You implement pre-deployment gates.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead use implement continuous integration.

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

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

Reference:

<https://azuredavolabs.com/labs/vstsextrnd/whitesource/>

NO.113 You have a build pipeline in Azure Pipelines that occasionally fails.

You discover that a test measuring the response time of an API endpoint causes the failures.

You need to prevent the build pipeline from failing due to The test.

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

NOTE: Each correct selection is worth one point

- A.** Enable Test Impact Analysis (TIA).
- B.** Enable test slicing.
- C.** Clear Flaky tests included in test pass percentage
- D.** Set Flaky test detection to Off
- E.** Manually mark the test as flaky.

Answer: C E

Reference:

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

NO.114 You have an Azure subscription. The subscription contains virtual machines that run either Windows Server or Linux.

You plan to use Prometheus to monitor performance metrics.

You need to integrate Prometheus and Azure Monitor.

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

NOTE: Each correct selection is worth one point.

- A.** Install a Prometheus server on a Windows virtual machine in Azure.
- B.** On each virtual machine, expose the metrics endpoint.
- C.** On each virtual machine, enable the Azure Diagnostics extension.
- D.** On each virtual machine, enable the containerized agent for Azure Monitor.
- E.** Expose a virtual network service endpoint for Azure Storage.
- F.** Install a Prometheus server on a Linux virtual machine in Azure.

Answer: A B

NO.115 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.

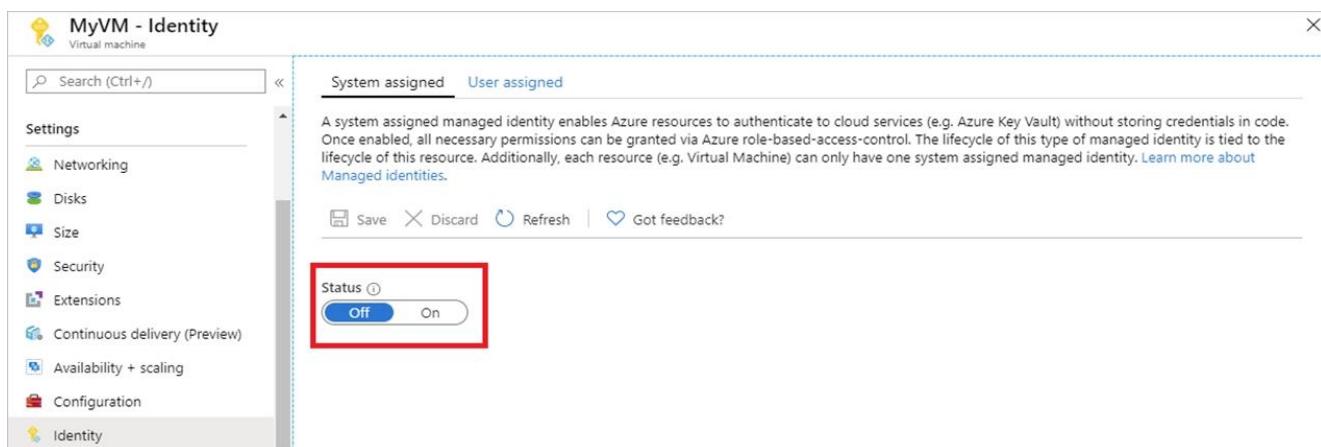
Answer:

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>

NO.116 You need to ensure that an Azure web app named az400-9940427-main supports rolling upgrades. The solution must ensure that only 10 percent of users who connect to az400-9940427-main use update versions of the app.

The solution must minimize administrative effort.

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

Answer:

See solution below.

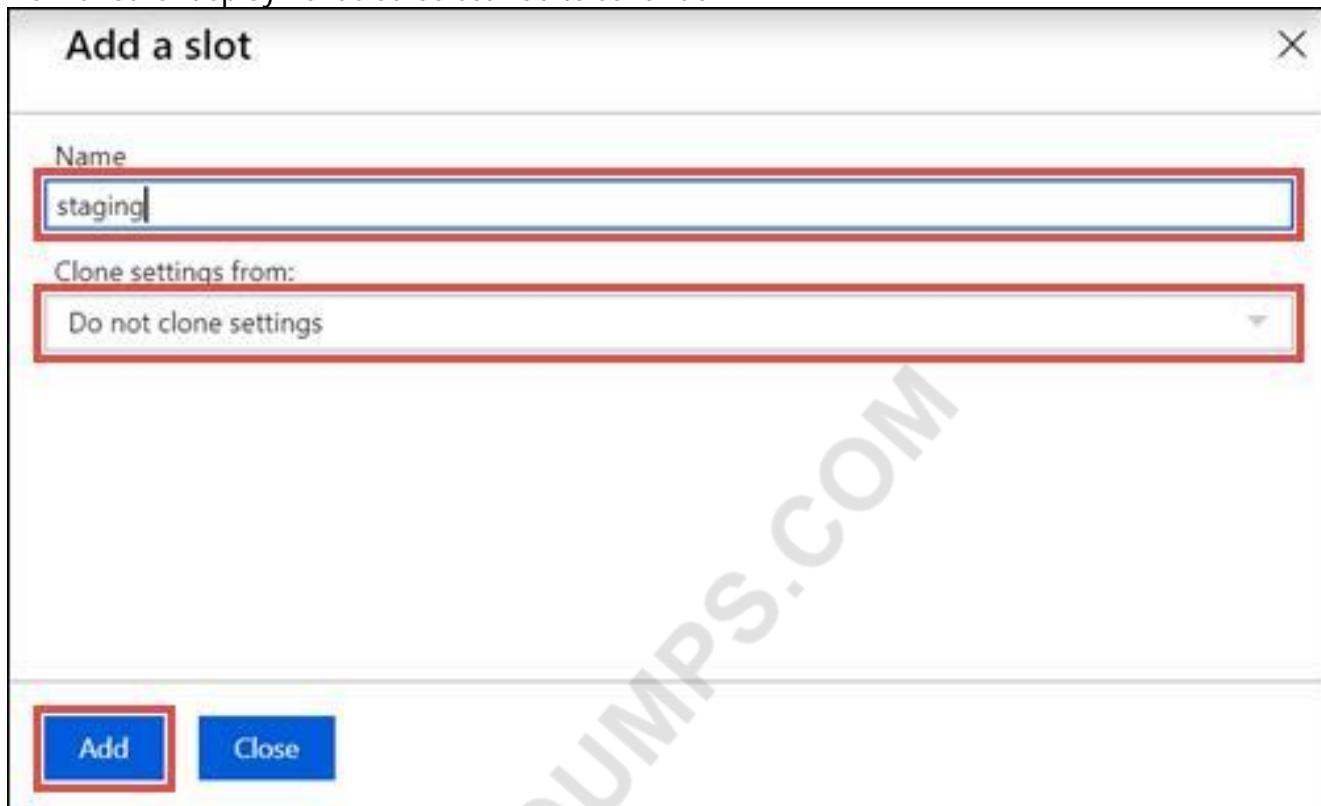
Explanation

Set up staging environments in Azure App Service

1. Open Microsoft Azure Portal
2. Log into your Azure account, select your app's resource page, in the left pane, select Deployment slots > Add Slot.

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

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. By default, Traffic % is set to 0 for the new slot, with all customer traffic routed to the production slot.

5. Select the new deployment slot to open that slot's resource page.

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

6. Change TRAFFIC % to 10

References:

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

NO.117 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":  
        "details": [  
          "Append",  
          "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":  
        "details": [  
          {"  
            "field": "tags['organization']",  
            "value": "Contoso"  
          }  
        ]  
    }  
  }  
}
```

Explanation

```

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

```

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>

NO.118 You plan to provision a self-hosted Linux agent

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

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

Answer: B

Explanation

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

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/y2-linux>

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

NO.119 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

Reference:

<https://doi.org/10.5281/zenodo.1026031>

Open the file and click on the right mouse button to bring up the context menu.

NO.120 You create a Microsoft ASP.NET Core application.

You plan to use Azure Key Vault to provide secrets to the application as configuration data. You need to create a Key Vault access policy to assign secret permissions to the application. The solution must use the principle of least privilege.
Which secret permissions should you use?

- A. List only
- B. Get only
- C. Get and List

Answer: B

Explanation

Application data plane permissions:

- * Keys: sign
- * Secrets: get

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault>

NO.121 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

- * The builds must access an on-premises dependency management system.
- * The build outputs must be stored as Server artifacts in Azure DevOps.
- * The source code must be stored in a Git repository in Azure DevOps.

Solution: Configure the build pipeline to use a Hosted VS 2017 agent pool. Include the Java Tool Installer task in the build pipeline.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation

Instead use Octopus Tentacle.

References:

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

NO.122 You have a build pipeline in Azure Pipelines.

You create a Slack App Integration.

You need to send build notifications to a Slack channel named #Development.

What should you do first?

- A. Configure a service connection.
- B. Create a service hook subscription.
- C. Create a project-level notification.
- D. Create a global notification.

Answer: B

Explanation

Create a service hook for Azure DevOps with Slack to post messages to Slack in response to events in your Azure DevOps organization, such as completed builds, code changes, pull requests, releases, work items changes, and more.

Note:

1. Go to your project Service Hooks page:

https://{{orgName}}/{{project_name}}/_settings/serviceHooks Select Create Subscription.

3. Choose the types of events you want to appear in your Slack channel.

4. Paste the Web Hook URL from the Slack integration that you created and select Finish.

5. Now, when the event you configured occurs in your project, a notification appears in your team's Slack channel.

Reference:

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

NO.123 Your company hosts a web application in Azure. The company uses Azure Pipelines for the build and release management of the application.

Stakeholders report that the past few releases have negatively affected system performance.

You configure alerts in Azure Monitor.

You need to ensure that new releases are only deployed to production if the releases meet defined performance baseline criteria in the staging environment first. What should you use to prevent the deployment of releases that fail to meet the performance baseline?

- A.** a trigger
- B.** an Azure function
- C.** a gate
- D.** an Azure Scheduler job

Answer: C

NO.124 You administer an Azure DevOps project that includes package feeds.

You need to ensure that developers can unlist and deprecate packages. The solution must use the principle of least privilege.

Which access level should you grant to the developers?

- A.** Collaborator
- B.** Contributor
- C.** Owner

Answer: B

Explanation

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.

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

Reference:

<https://docs.microsoft.com/en-us/azure/devops/artifacts/feeds/feed-permissions>

NO.125 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

- * The builds must access an on-premises dependency management system.
- * The build outputs must be stored as Server artifacts in Azure DevOps.
- * The source code must be stored in a Git repository in Azure DevOps.

Solution: Configure the build pipeline to use a Hosted Ubuntu agent pool. Include the Java Tool Installer task in the build pipeline. Does this meet the goal?

A. Yes

B. No

Answer: A

NO.126 You are designing the development process for your company.

You need to recommend a solution for continuous inspection of the company's code base to locate common code patterns that are known to be problematic.

What should you include in the recommendation?

A. Microsoft Visual Studio test plans

B. Gradle wrapper scripts

C. SonarCloud analysis

D. the JavaScript task runner

Answer: C

Explanation

SonarCloud is a cloud service offered by SonarSource and based on SonarQube. SonarQube is a widely adopted open source platform to inspect continuously the quality of source code and detect bugs, vulnerabilities and code smells in more than 20 different languages.

Note: The SonarCloud Azure DevOps extension brings everything you need to have your projects analyzed on SonarCloud very quickly.

NO.127 Your company uses Team Foundation Server 2013 (TFS 2013).

You plan to migrate to Azure DevOps.

You need to recommend a migration strategy that meets the following requirements:

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

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

NOTE: Each correct selection is worth one point.

On the TFS server:

- | |
|--|
| Install the TFS Java SDK. |
| Upgrade TFS to the most recent RTW release. |
| Upgrade to the most recent version of PowerShell Core. |

To perform the migration:

- | |
|--------------------------------------|
| Copy the assets manually. |
| Use public API-based tools. |
| Use the TFS Database Import Service. |
| Use the TFS Integration Platform. |

Answer:

On the TFS server:

- | |
|--|
| Install the TFS Java SDK. |
| Upgrade TFS to the most recent RTW release. |
| Upgrade to the most recent version of PowerShell Core. |

To perform the migration:

- | |
|--------------------------------------|
| Copy the assets manually. |
| Use public API-based tools. |
| Use the TFS Database Import Service. |
| Use the TFS Integration Platform. |

Explanation

On the TFS server:

- Install the TFS Java SDK.
- Upgrade TFS to the most recent RTW release.**
- Upgrade to the most recent version of PowerShell Core.

To perform the migration:

- Copy the assets manually.
- Use public API-based tools.
- Use the TFS Database Import Service.**
- Use the TFS Integration Platform.

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

NO.128 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

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

You have a policy stating that approvals must occur within eight hours.

You discover that deployment fail if the approvals take longer than two hours.

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

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

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Use Pre-deployments conditions instead.

Use a gate instead of an approval instead.

References:

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

NO.129 You plan to use Azure Kubernetes Service (AKS) to host containers deployed from images hosted in a Docker Trusted Registry.

You need to recommend a solution for provisioning and connecting to AKS. The solution must ensure

that AKS is RBAC-enabled and uses a custom service principal.

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

Commands

kubectl create
az role assignment create
az aks get-credentials
az ad sp create-for-rbac
az aks create

Answer Area

1
2
3

<
>
^
▼

Answer:

Commands

kubectl create
az role assignment create
az aks get-credentials
az ad sp create-for-rbac
az aks create

Answer Area

1 az aks create
2 az ad sp create-for-rbac
3 kubectl create

<
>
^
▼

Explanation

`az aks create`

`az ad sp create-for-rbac`

`kubectl create`

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.ContainerReg`

istry/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>

NO.130 You have a web app that connects to an Azure SQL Database named db1.

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

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

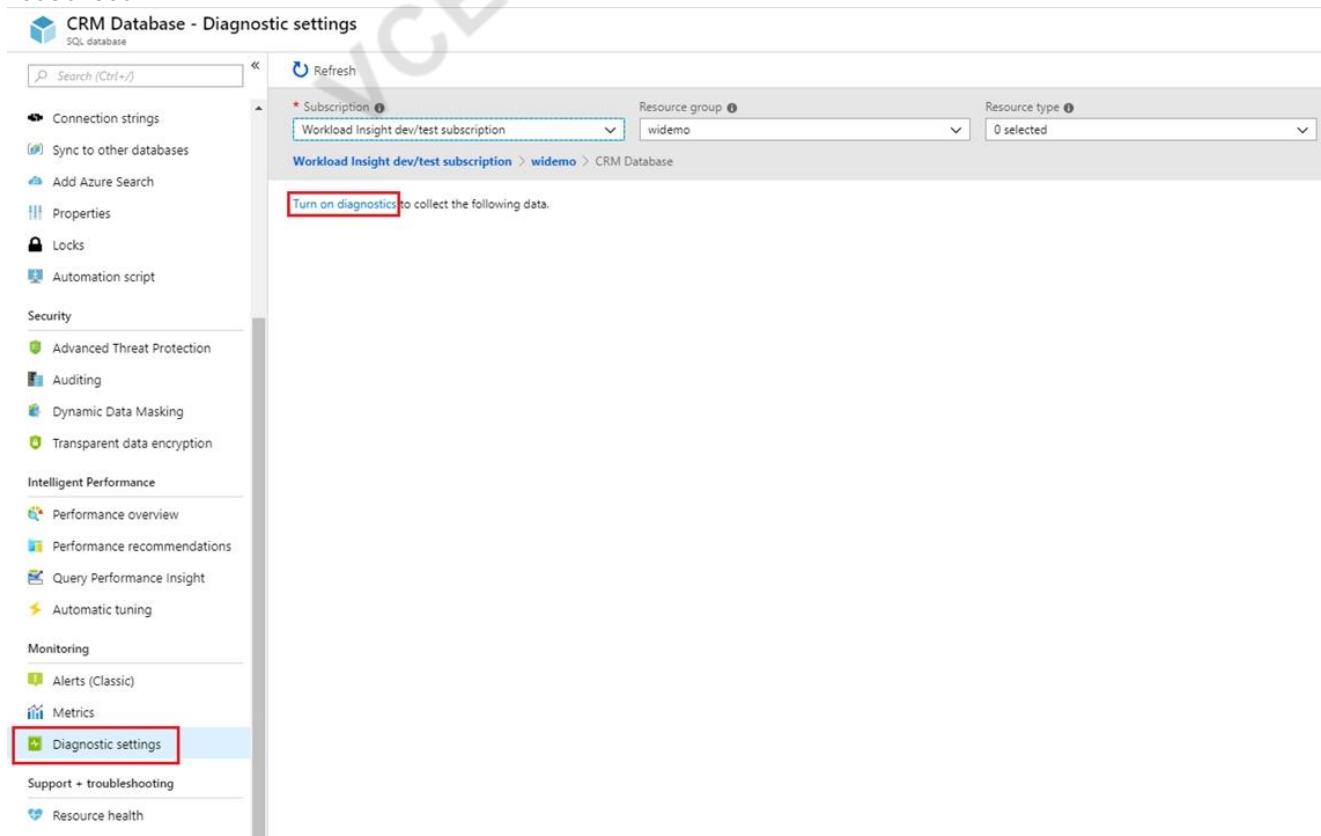
Answer:

See solution below.

Explanation

To enable streaming of diagnostic telemetry for a single or a pooled database, follow these steps:

1. Go to Azure SQL database resource.
2. Select Diagnostics settings.
3. Select Turn on diagnostics if no previous settings exist, or select Edit setting to edit a previous setting. You can create up to three parallel connections to stream diagnostic telemetry.
4. Select Add diagnostic setting to configure parallel streaming of diagnostics data to multiple resources.



5. Enter a setting name for your own reference.
6. Select a destination resource for the streaming diagnostics data: Archive to storage account, Stream to an event hub, or Send to Log Analytics.
7. For the standard, event-based monitoring experience, select the following check boxes for database diagnostics log telemetry: QueryStoreRuntimeStatistics

VCEDUMPS.COM

Diagnostics settings

X

Save Discard Delete

* Name
service

Archive to a storage account

Stream to an event hub

Send to Log Analytics

Subscription

Workload Insight dev/test subscription

Log Analytics Workspace

sqlanalytics356 (westcentralus)

LOG

SQLInsights

AutomaticTuning

QueryStoreRuntimeStatistics

QueryStoreWaitStatistics

Errors

DatabaseWaitStatistics

Timeouts

Blocks

Deadlocks

METRIC

Basic

8. For an advanced, one-minute-based monitoring experience, select the check box for Basic metrics.
9. Select Save.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export>

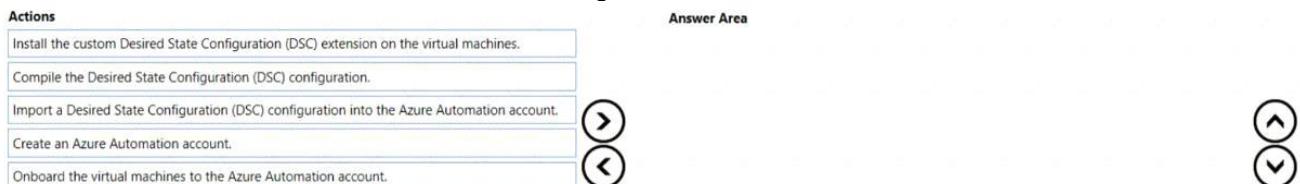
NO.131 You have an Azure DevOps organization named Contoso.

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.

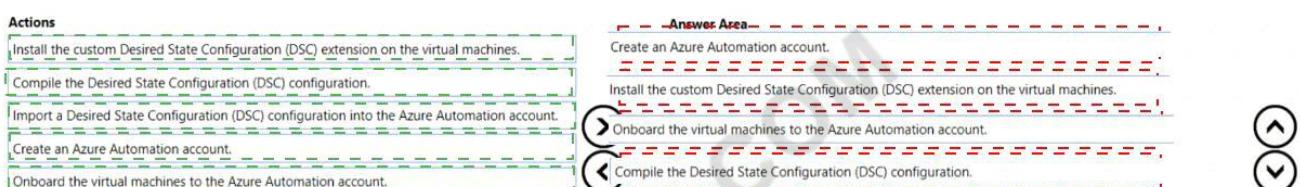
You need to ensure that the web server configurations pin the virtual machines is maintained automatically.

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:



Explanation

Create an Azure Automation account.

Install the custom Desired State Configuration (DSC) extension on the virtual machines.

Onboard the virtual machines to the Azure Automation account.

Complete the Desired State Configuration (DSC) configuration.

Step1: Create an Azure Automation account.

An Azure Automation account is required.

Step 2: Install the custom Desired State Configuration (DSC) extension on the virtual machines Under the hood, and without an administrator having to remote into a VM, the Azure VM Desired State Configuration extension registers the VM with Azure Automation State Configuration.

Step 3: Onboard the virtual machines to the Azure Automation account.

Step 4: Complete the Desired State Configuration (DSC) configuration.

Create a DSC configuration.

Reference:

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

NO.132 You plan to create a project in Azure DevOps. Multiple developers will work on the project. The developers will work offline frequently and will require access to the full project history while they are offline.

Which version control solution should you use?

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

Answer: D

Explanation

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

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

Reference:

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

NO.133 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>

NO.134 You are designing the security validation strategy for a project in Azure DevOps.

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

What should you use?

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

Answer: D

Explanation

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

NO.135 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

Explanation

Scenarios and use cases for gates include:

- * Quality validation. Query metrics from tests on the build artifacts such as pass rate or code coverage and deploy only if they are within required thresholds.

Use Quality Gates to integrate monitoring into your pre-deployment or post-deployment. This ensures that you are meeting the key health/performance metrics (KPIs) as your applications move from dev to production and any differences in the infrastructure environment or scale is not negatively impacting your KPIs.

Note: Gates allow automatic collection of health signals from external services, and then promote the release when all the signals are successful at the same time or stop the deployment on timeout.

Typically, gates are used in connection with incident management, problem management, change management, monitoring, and external approval systems.

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/continuous-monitoring>

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

NO.136 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.

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

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

NOTE: Each correct selection is worth one point.

The pipeline contains

	▼
one stage	
two stages	
three stages	
four stages	
five stages	

Build_vm contains

	▼
one job	
two jobs	
three jobs	
four jobs	
five jobs	

Answer:

The pipeline contains

	▼
one stage	
two stages	
three stages	
four stages	
five stages	

Build_vm contains

	▼
one job	
two jobs	
three jobs	
four jobs	
five jobs	

Explanation

The pipeline contains

	▼
one stage	
two stages	
three stages	
four stages	
five stages	

Build_vm contains

	▼
one job	
two jobs	
three jobs	
four jobs	
five jobs	

Reference:

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

NO.137 You need to find and isolate shared code. The shared code will be maintained in a series of packages.

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

Actions

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

Answer Area

Answer:

Actions

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

Answer Area

- Create a dependency graph for the application.
- Group the related components.
- Assign ownership to each component group.

Explanation

Create a dependency graph for the application.

Group the related components.

Assign ownership to each component group.

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>

NO.138 Your company is concerned that when developers introduce open source libraries, it creates licensing compliance issues.

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

What should you use?

- A.** Microsoft Visual SourceSafe
- B.** PDM
- C.** WhiteSource
- D.** OWASP ZAP

Answer: C

Explanation

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

Azure DevOps integration with WhiteSource Bolt will enable you to:

- * 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/>

NO.139 Your company uses cloud-hosted Jenkins for builds.

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

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

Each correct answer selection is worth one point

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

Answer: A B E

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-foundation-serv>

NO.140 You plan to create an image that will contain a .NET Core application.

You have a Dockerfile file that contains the following code. (Line numbers are included for reference only.)

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

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

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

Answer: C

Explanation

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

NO.141 You need to recommend a solution for deploying charts by using Helm and Title to Azure Kubemets Service (AKS) in an RBAC-enabled cluster.

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

Commands

Answer Area

helm install

kubectl create

helm completion

helm init

helm serve



Answer:

Commands`helm install``kubectl create``helm completion``helm init``helm serve`**Answer Area**`kubectl create``helm init``helm install`

Explanation

Answer Area`kubectl create``helm init``helm install`

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

NO.142 You manage build pipelines and deployment pipelines by using Azure DevOps.

Your company has a team of 500 developers. New members are added continually to the team. You need to automate the management of users and licenses whenever possible. Which task must you perform manually?

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

Answer: B

Explanation

References:

[https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/migrate-to-group-based-resource-management](https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/migrate-to-group-based-resource-management?view=azure-devops)

<https://docs.microsoft.com/en-us/rest/api/azure/devops/memberentitlementmanagement/?view=azure-devops-resources>

NO.143 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

Create an agent pool

Create a deployment group

Execute the Azure Pipelines Agent extension to the virtual machines

Add and configure a deployment group job for the pipeline

Step 1: Create an agent pool

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

Step 2: Create a deployment group

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

Step 3: Execute the Azure Pipelines Agent extension to the virtual machines
Install the Azure Pipelines Agent Azure VM extension
Step 4: Add and configure a deployment group job for the pipeline
Tasks that you define in a deployment group job run on some or all of the target servers, depending on the arguments you specify for the tasks and the job itself.

Reference:

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

NO.144 Your company has a project in Azure DevOps.

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

The templates will reference secrets stored in Azure Key Vault.

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

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

NOTE: Each correct selection is worth one point.

Configurations**Answer Area**

an Azure Key Vault access policy

Restrict access to delete the key vault:

a personal access token (PAT)

Restrict access to the secrets in Key Vault by using:

RBAC

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

an Azure Key Vault access policy

Restrict access to delete the key vault: RBAC

a personal access token (PAT)

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

RBAC

Explanation

Restrict access to delete the key vault: RBAC

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

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>

NO.145 You are creating a build pipeline in Azure Pipelines.

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

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

What should you do?

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

Answer: B

NO.146 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

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>

NO.147 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.

You need to recommend changes to reduce the accumulated technical debt.

Solution: You recommend increasing the test coverage.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead reduce the code complexity.

Reference:

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

NO.148 As part of your application build process, you need to deploy a group of resources to Azure by using an Azure Resource Manager template located on GitHub.

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

Actions	Answer Area
Create a package.	>
Add an Azure Resource Group Deployment task.	
Create a job agent.	
Create a release pipeline.	
Set the template parameters.	

Answer:



Explanation

Create a release pipeline.

Add an Azure Resource Group Deployment task.

Set the template parameters.

Step 1: Create a release pipeline

You need to create a new pipeline.

You can integrate Azure Resource Manager templates (ARM templates) with Azure Pipelines for continuous integration and continuous deployment (CI/CD).

Step 2: Add an Azure Resource Group Deployment task

Step 3: Set the template parameters

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/add-template-to-azure-pipelines>

NO.149 You have a free tier of an Azure DevOps organization named Contoso. Contoso contains 10 private projects.

Each project has multiple jobs with no dependencies.

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

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

What should you do?

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

Answer: A

Explanation

<https://docs.microsoft.com/en-us/azure/devops/organizations/billing/buy-more-build-vs?view=azure-devops#self>

NO.150 You have an Azure DevOps organization named Contoso that contains a project named Project 1.

You provision an Azure key vault name 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.

Answer: B

Explanation

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

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

Reference:

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

NO.151 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 organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 that is configured for autoscaling.

You have a project in Azure DevOps named Project1. Project1 is used to build a web app named App1 and deploy App1 to VMSS1.

You need to ensure that an email alert is generated whenever VMSS1 scales in or out.

Solution: From Azure DevOps, configure the Notifications settings for Project1.

Does this meet the goal?

- A.** Yes
- B.** No

Answer: A

NO.152 You create an alert rule in Azure Monitor as shown in the following exhibit.

Which action will trigger an alert?

- A. a failed attempt to delete the ASP-9bb7 resource
- B. a change to a role assignment for the ASP-9bb7 resource
- C. a successful attempt to delete the ASP-9bt>7 resource
- D. a failed attempt to scale up the ASP-9bb7 resource

Answer: A

NO.153 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You integrate a cloud-hosted Jenkins server and a new Azure Dev Ops deployment.

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

Solution: You create an email subscription to an Azure DevOps notification.

Does this meet the goal?

- A. Yes
- B. NO

Answer: B

Explanation

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

References:

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

NO.154 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:

The screenshot shows the 'Advanced Data Security' configuration page for a SQL server named 'vanazuresqldbserver'. The left sidebar lists various management options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Quick start, Failover groups, Manage Backups, Active Directory admin, SQL databases, SQL elastic pools, Deleted databases, Import/Export history, DTU quota, Properties, Locks, Export template, and Security. The 'Advanced Data Security' option is highlighted with a red box. The main pane shows 'ADVANCED DATA SECURITY' set to 'ON'. Under 'VULNERABILITY ASSESSMENT SETTINGS', there are sections for Subscription, SQL DB Content, and Storage account. Under 'Periodic recurring scans', it is also set to 'ON'. There is a section for 'Send scan reports to' with a text input field and a checkbox for 'Also send email notification to admins and subscription owners' which is checked. A large red box highlights the 'ADVANCED THREAT PROTECTION SETTINGS' section, which includes fields for 'Send alerts to' (containing 'Email addresses') and another checkbox for 'Also send email notification to admins and subscription owners' which is also checked. Below this, there is a section for 'Advanced Threat Protection types' set to 'All'.

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/sql/database/threat-detection-configure>

NO.155 You have an Azure Resource Manager template that deploys a multi-tier application. You need to prevent the user who performs the deployment from viewing the account credentials and connection strings used by the application.

What should you use?

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

Answer: D

Explanation

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

References:

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

NO.156 Your company has four projects. The version control requirements for each project are shown in the following table.

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

You plan to use Azure Repos for all the projects.

Which version control system should you use for each project? To answer, drag the appropriate version control systems to the correct projects. Each version control system may be used once, more than once, or not at all.

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

NOTE: Each correct selection is worth one point.

Version Control Systems**Answer Area**

Git

Project 1:

Perforce

Project 2:

Subversion

Project 3:

Team Foundation Version Control

Project 4:

Answer:**Version Control Systems****Answer Area**

Git

Project 1: Team Foundation Version Control

Perforce

Project 2: Team Foundation Version Control

Subversion

Project 3: Git

Team Foundation Version Control

Project 4: Team Foundation Version Control

Explanation

1 -> TFVS Refer :

<https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/control-access-team-foundation-version-control?view=>

2 -> TFVS Refer :

<https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/add-check-policies?view=azure-devops>

3 -> Git Refer :

<https://docs.microsoft.com/en-us/azure/devops/repos/git/share-your-code-in-git-xcode?view=azure-devops>

4 -> TFVS Refer

<https://docs.microsoft.com/en-us/azure/devops/organizations/security/permissions?view=azure-devops#tfvc>

NO.157 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage a project in Azure DevOps.

You need to prevent the configuration of the project from changing over time.

Solution: Add a code coverage step to the build pipelines.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead implement Continuous Assurance for the project.

Reference:

<https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html>

NO.158 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

NO.159 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. managed identities in Azure Active Directory (Azure AD)

B. personal access tokens (PATs) in Azure DevOps

C. user accounts in Azure Active Directory (Azure AD)

D. Alternate credentials in Azure DevOps

Answer: B

Explanation

Personal access tokens (PATs) give you access to Azure DevOps and Team Foundation Server (TFS), without using your username and password directly. These tokens have an expiration date from when they're created.

You can restrict the scope of the data they can access. Use PATs to authenticate if you don't already have SSH keys set up on your system or if you need to restrict the permissions that are granted by the credential.

Reference:

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

NO.160 You have a private distribution group that contains provisioned and unprovisioned devices.

You need to distribute a new iOS application to the distribution group by using Microsoft Visual Studio App Center.

What should you do?

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

B. Register the devices on the Apple Developer portal.

- C. Create an active subscription in App Center Test.
- D. Add the device owner to the organization in App Center.

Answer: B

Explanation

When releasing an iOS app signed with an ad-hoc or development provisioning profile, you must obtain tester's device IDs (UDIDs), and add them to the provisioning profile before compiling a release. When you enable the distribution group's Automatically manage devices setting, App Center automates the before mentioned operations and removes the constraint for you to perform any manual tasks. As part of automating the workflow, you must provide the user name and password for your Apple ID and your production certificate in a .p12 format.

App Center starts the automated tasks when you distribute a new release or one of your testers registers a new device. First, all devices from the target distribution group will be registered, using your Apple ID, in your developer portal and all provisioning profiles used in the app will be generated with both new and existing device ID. Afterward, the newly generated provisioning profiles are downloaded to App Center servers.

References:

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

NO.161 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You have a policy stating that approvals must occur within eight hours.

You discover that deployment fail if the approvals take longer than two hours.

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

Solution: From Pre-deployment conditions, you modify the Time between re-evaluation of gates option.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

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

NO.162 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

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>

NO.163 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You use a Git repository for applications source control.

You need to implement a pull request strategy that reduces the history volume in the master branch.

Solution: You implement a pull request strategy that uses a three-way merge.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead use fast-forward merge.

Note:

No fast-forward merge - This option merges the commit history of the source branch when the pull request closes and creates a merge commit in the target branch.

Reference:

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

NO.164 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: B

Explanation

<https://azuredevopslabs.com/labs/vstsextend/teams/>

NO.165 You plan to deploy a runbook that will create Azure AD user accounts.

You need to ensure that runbooks can run the Azure PowerShell cmdlets for Azure Active Directory. To complete this task, sign in to the Microsoft Azure portal.

Answer:

See solution below.

Explanation

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

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

1. Log in to the Azure portal as the service administrator for the Azure subscription you want to manage using Azure Automation. You can find this user by logging in to the Azure portal as any user with access to this Azure subscription, then clicking Settings, then Administrators.



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

settings

SUBSCRIPTIONS MANAGEMENT CERTIFICATES ADMINISTRATORS AFFINITY GROUPS USAGE

SUBSCRIPTION	SUBSCRIPTION ID	ACCOUNT ADMINISTRATOR	DIRECTORY
Windows Azure MSDN - Visual Studio Ultimate	[REDACTED]	[REDACTED]	Joe Levy

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

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

1. In the Azure portal click on Active Directory service.



2. Click the directory name that is associated with this Azure subscription.
3. Click on the Users tab and then click the Add User button.
4. For type of user, select "New user in your organization." Enter a username for the user to create.
5. Fill out the user's profile. For role, pick "User." Don't enable multi-factor authentication. Multi-

factor accounts cannot be used with Azure Automation.

6. Click Create.

7. Jot down the full username (including part after @ symbol) and temporary password.

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

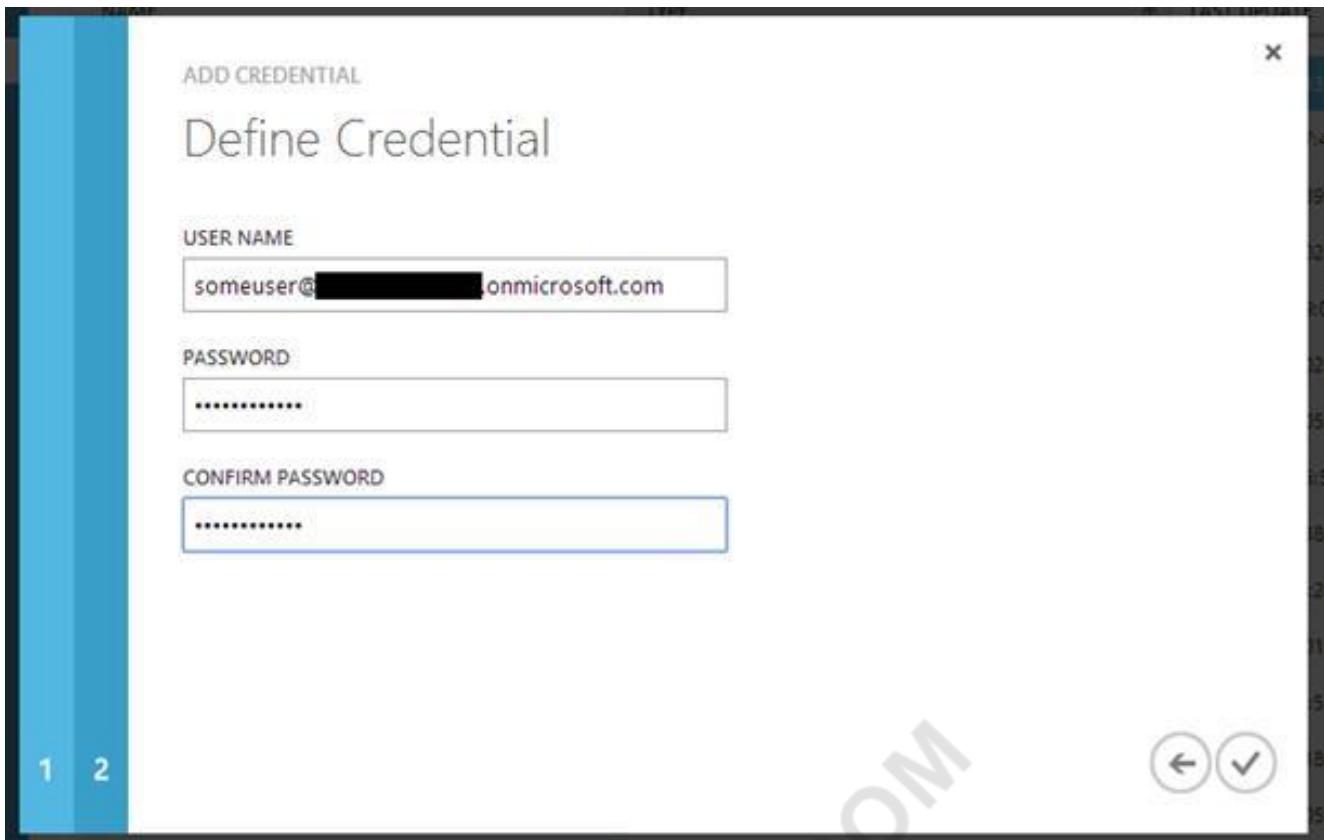
1. Click on Settings (bottom Azure tab under StorSimple)



2. Click Administrators

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

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



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

References:

<https://azure.microsoft.com/sv-se/blog/azure-automation-authenticating-to-azure-using-azure-active-directory/>

NO.166 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>

NO.167 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 Area

Production code: Master
 Feature
 Develop

Preproduction code: Master
 Feature
 Develop

Answer:

Answer Area

Production code: Master
 Feature
 Develop

Preproduction code: Master
 Feature
 Develop

Explanation

Answer Area

Production code: Master

Preproduction code: Develop

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>

NO.168 You are implementing a package management solution for a Node.js application by using Azure Artifacts.

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

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

Files

The .npmrc file in the project

The .npmrc file in the user's home folder

The Package.json file in the project

The Project.json file in the project

Answer Area

Registry information: File

Credentials: File

Answer:**Files**

The .npmrc file in the project

The .npmrc file in the user's home folder

The Package.json file in the project

The Project.json file in the project

Answer Area

Registry information: The .npmrc file in the project

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

Explanation

Feed registry information: **The .npmrc file in the project**

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

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>

NO.169 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.

Values	Answer Area
Configuration	Value MyDsc {
DependsOn	Node 'Server1' {
File	Value MyConfigDetail {
IncludeAllSubFeature	Ensure = 'Present'
WindowsFeature	Name = 'Web-Server'

Answer:

Values

- Configuration
- DependsOn
- File
- IncludeAllSubFeature
- WindowsFeature

Answer Area

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

Explanation**Answer Area**

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

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>

NO.170 You use Azure Pipelines to manage build pipelines. GitHub to store source code, and Dependabot to manage dependencies.

You have an app named App1.

Dependabot detects a dependency in App1 that requires an update.

What should you do first to apply the update?

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

Answer: C

Explanation

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

- * 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 Reference:

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

NO.171 You have a private distribution group that contains provisioned and unprovisioned devices.

You need to distribute a new iOS application to the distribution group by using Microsoft Visual Studio App Center.

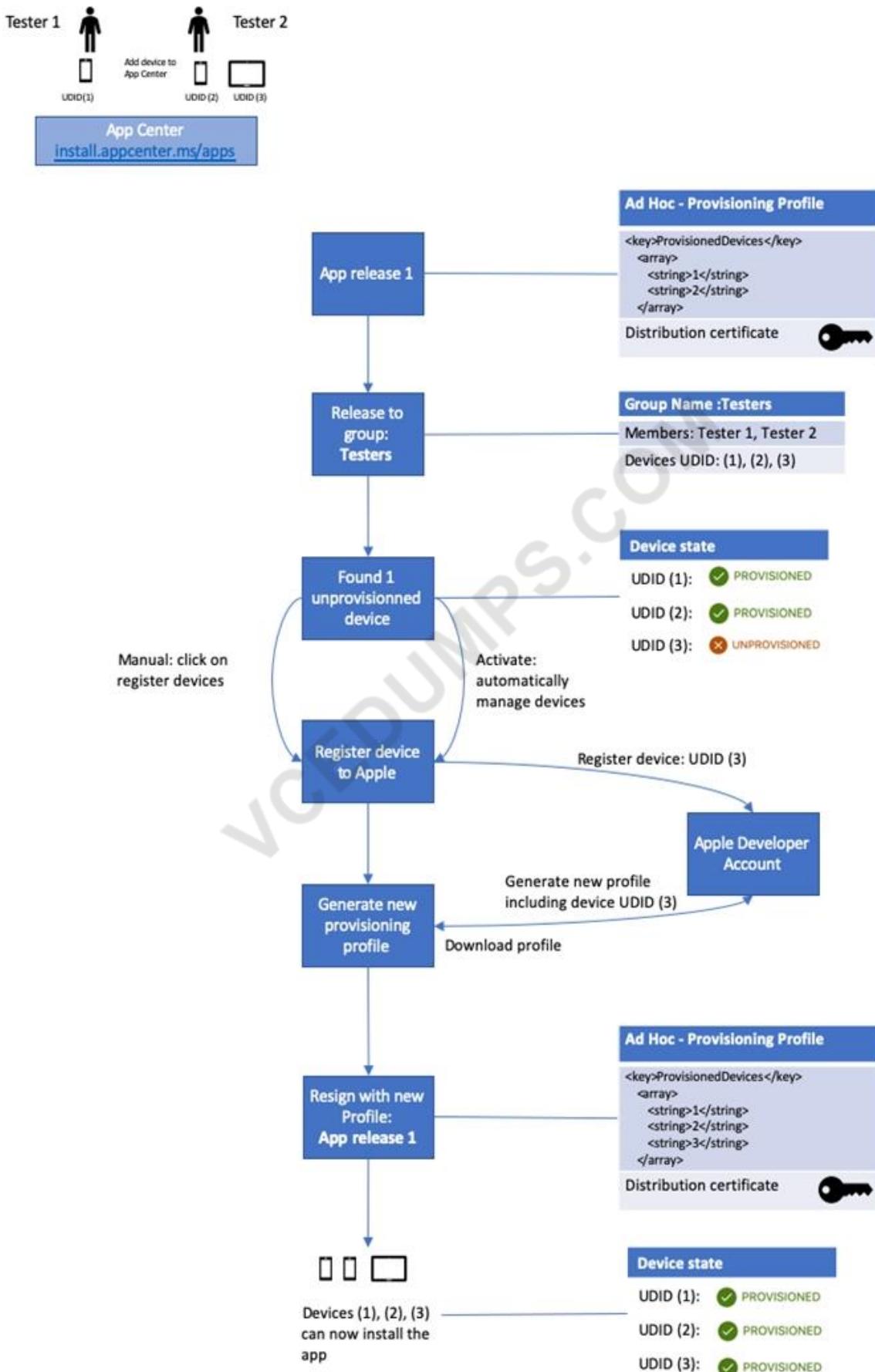
What should you do?

- A.** Select Register devices and sign my app.
- B.** Generate a new .p12 file for each device.
- C.** Create an active subscription in App Center Test.
- D.** Add the device owner to the collaborators group.

Answer: A

Explanation

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



Reference:

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

NO.172 You are configuring an Azure DevOps deployment pipeline. The deployed application will authenticate to a web service by using a secret stored in an Azure key vault. You need to use the secret in the deployment pipeline. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Add an app registration in Azure Active Directory (Azure AD).	
Configure an access policy in the key vault.	
Export a certificate from the key vault.	
Add an Azure Resource Manager service connection to the pipeline.	▶
Generate a self-signed certificate.	◀
Create a service principal in Azure Active Directory (Azure AD).	

↑
↓
↑
↓

Answer:

Actions	Answer Area
Add an app registration in Azure Active Directory (Azure AD).	
Configure an access policy in the key vault.	
Export a certificate from the key vault.	
Add an Azure Resource Manager service connection to the pipeline.	▶
Generate a self-signed certificate.	◀
Create a service principal in Azure Active Directory (Azure AD).	

↑
↓
↑
↓

Explanation

Creating a service principal

Creating a key vault

Check the Azure Pipeline

NO.173 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.

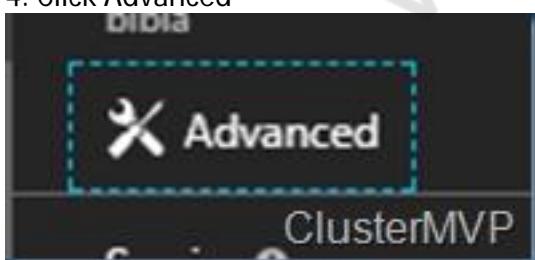
To complete this task, sign in to the Microsoft Azure portal.

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://robertsmitsmit.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>

NO.174 Your company develops a client banking application that processes a large volume of data.

Code quality is an ongoing issue for the company. Recently, the code quality has deteriorated because of an increase in time pressure on the development team.

You need to implement static code analysis.

During which phase should you use static code analysis?

- A.** build
- B.** production release
- C.** staging
- D.** integration testing

Answer: D

Explanation

The Secure Development Lifecycle (SDL) Guidelines recommend that teams perform static analysis during the implementation phase of their development cycle.

Note: The company should focus in particular on the implementation of DevOps tests to assess the quality of the software from the planning stage to the implementation phase of the project.

References:

<https://secdevtools.azurewebsites.net/>

NO.175 Your company has a project in Azure DevOps for a new application. The application will be deployed to several Azure virtual machines that run Windows Server 2016.

You need to recommend a deployment strategy for the virtual machines. The strategy must meet the following requirements:

- * Ensure that the virtual machines maintain a consistent configuration.
- * Minimize administrative effort to configure the virtual machines

What should you include in the recommendation?

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

Answer: B

Explanation

The Custom Script Extension downloads and executes scripts on Azure virtual machines. This extension is useful for post deployment configuration, software installation, or any other configuration or management tasks. Scripts can be downloaded from Azure storage or GitHub, or provided to the Azure portal at extension run time. The Custom Script Extension integrates with Azure Resource Manager templates, and can be run using the Azure CLI, PowerShell, Azure portal, or the Azure Virtual Machine REST API.

References:

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

NO.176 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 ACM.

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

Answer: A

Explanation

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

NO.177 You are integrating Azure Pipelines and Microsoft Teams.

You install the Azure Pipelines app in Microsoft Teams.

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

You subscribe to Project1 in Microsoft Teams.

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

What should you do first?

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

Answer: A

Explanation

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

@azure pipelines subscribe [project url]

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

For example:

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

Reference:

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

NO.178 You use Azure Artifacts to host NuGet packages that you create.

You need to make one of the packages available to anonymous users outside your organization. The solution must minimize the number of publication points.

What should you do?

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

Answer: A

Explanation

Azure Artifacts introduces the concept of multiple feeds that you can use to organize and control access to your packages.

Packages you host in Azure Artifacts are stored in a feed. Setting permissions on the feed allows you to share your packages with as many or as few people as your scenario requires.

Feeds have four levels of access: Owners, Contributors, Collaborators, and Readers.

References:

<https://docs.microsoft.com/en-us/azure/devops/artifacts/feeds/feed-permissions?view=vsts&tabs=new-nav>

NO.179 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.

Components**Answer Area**

A deployment group

Ten virtual machines hosted in Azure:

A management group

Ten virtual machines hosted in
an on-premises data center environment:

Application roles

Answer:**Components****Answer Area**

A deployment group

Ten virtual machines hosted in Azure:

A management group

A deployment group

A resource group

Ten virtual machines hosted in
an on-premises data center environment:

A deployment group

Application roles

Explanation

Ten virtual machines hosted in Azure:

A deployment group

Ten virtual machines hosted in an on-premises data center environment:

A deployment group

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>

NO.180 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: B

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 is 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://azuredovopslabs.com/labs/vstsextend/sonarqube/>

NO.181 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

Explanation

Instead use implement continuous integration.

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

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

Reference:

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

NO.182 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

Explanation

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

NO.183 Your company has a project in Azure DevOps for a new web application.

The company uses Service Now for change management.

You need to ensure that a change request is processed before any components can be deployed to the production environment.

What are two ways to integrate into the Azure DevOps release pipeline? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Define a deployment control that invokes the Service Now SOAP API.
- B. Define a post deployment gate after the deployment to the QA stage.
- C. Define a deployment control that invokes the ServiceNow REST API.
- D. Define a pre deployment gate before the deployment to the Prod stage.

Answer: A B

Explanation

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

NO.184 Your company plans to use an agile approach to software development.

You need to recommend an application to provide communication between members of the development team who work in locations around the world. The applications must meet the following requirements:

- * Provide the ability to isolate the members of different project teams into separate communication channels and to keep a history of the chats within those channels.
- * Be available on Windows 10, Mac OS, iOS, and Android operating systems.
- * Provide the ability to add external contractors and suppliers to projects.
- * Integrate directly with Azure DevOps.

What should you recommend?

- A. Microsoft Project
- B. Bamboo
- C. Microsoft Lync
- D. Microsoft Teams

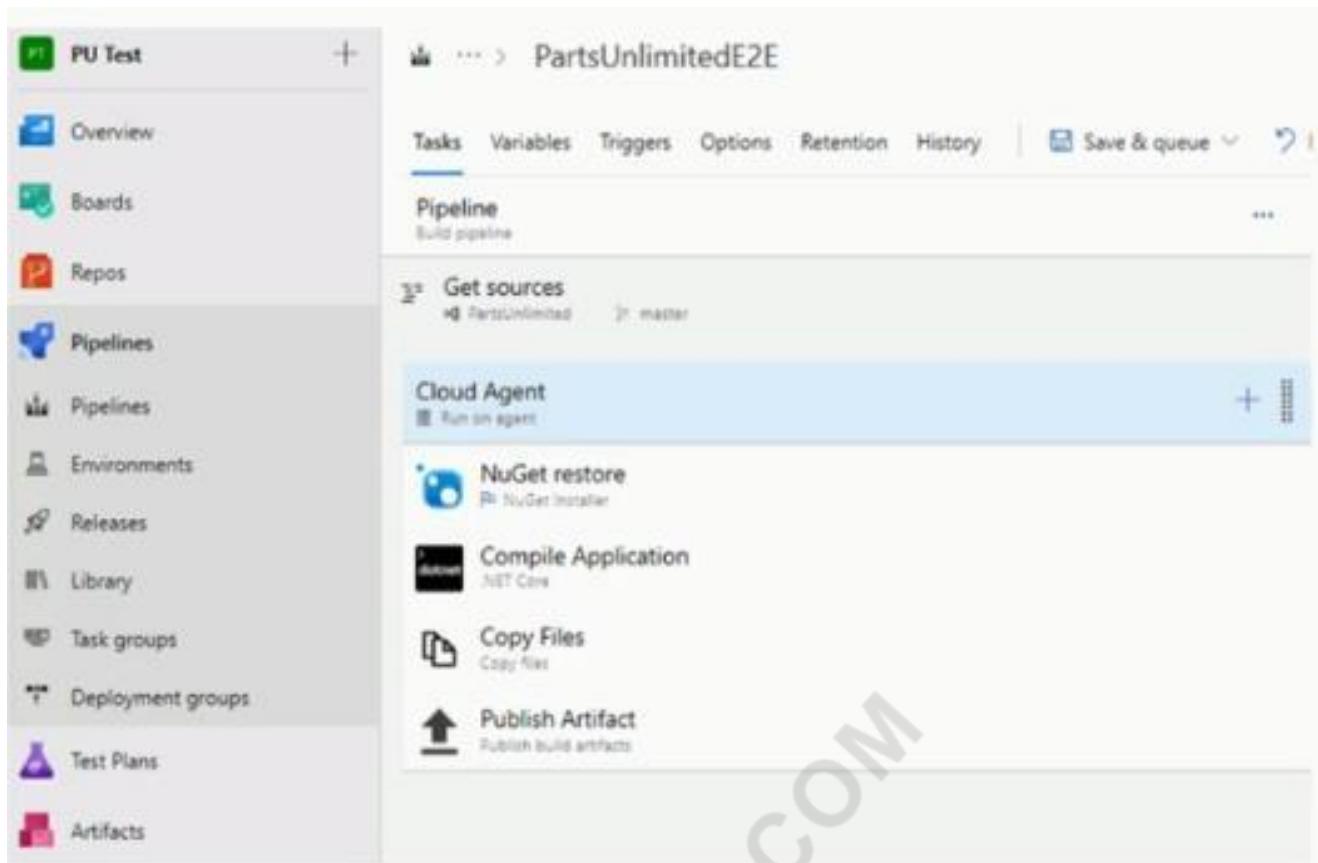
Answer: D

Explanation

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

References: <https://searchunifiedcommunications.techtarget.com/definition/Microsoft-Teams>

NO.185 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 Area

The pipeline has job(s).

The pipeline has task(s).

Answer:

Answer Area

The pipeline has job(s).

The pipeline has task(s).

Explanation

The pipeline has  job(s).

0
1
4

The pipeline has  task(s).

0
1
4

Box 1: 1

The Cloud agent job only.

Box 2: 4

The pipelines has the four tasks: NuGet restore, Compile Application, Copy Files, and Publish Artifact.

Reference:

<https://azuredevopslabs.com/labs/azuredevops/continuousintegration/>

NO.186 You have a multi-tier application. The front end of the application is hosted in Azure App Service. You need to identify the average load times of the application pages. What should you use?

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

Answer: B

NO.187 You are developing an iOS application by using Azure DevOps.

You need to test the application manually on 10 devices without releasing the application to the public.

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

NOTE: Each correct selection is worth one point.

- A. Create a Microsoft Intune device compliance policy.
- B. Deploy a certificate from an internal certification authority (CA) to each device.
- C. Register the application in the iTunes store.
- D. Onboard the devices into Microsoft Intune.
- E. Distribute a new release of the application.
- F. Register the IDs of the devices in the Apple Developer portal.

Answer: B F

Explanation

References:

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

NO.188 You have a project in Azure DevOps named Project1. Project1 contains a build pipeline named Pipe1 that builds an application named Appl.

You have an agent pool named Pool1 that contains a Windows Server 2019-based self-hosted agent. Pipe1 uses Pool1.

You plan to implement another project named Project2. Project2 will have a build pipeline named Pipe2 that builds an application named App2.

App1 and App2 have conflicting dependencies.

You need to minimize the possibility that the two build pipelines will conflict with each other. The solution must minimize infrastructure costs.

What should you do?

- A.** Create two container jobs.
- B.** Change the self-hosted agent to use Red Hat Enterprise Linux (RHEL) 8.
- C.** Add another self-hosted agent
- D.** Add a Docker Compose task to the build pipelines.

Answer: A

NO.189 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.

Components

Answer Area

A deployment group

Ten virtual machines hosted in Azure:

A management group

Ten virtual machines hosted in an on-premises data center environment:

A resource group

Application roles

Answer:

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

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>

NO.190 Your company has a release pipeline in an Azure DevOps project.

You plan to deploy to an Azure Kubernetes Services (AKS) cluster by using the Helm package and deploy task.

You need to install a service in the AKS namespace for the planned deployment.

Which service should you install?

- A.** Azure Container Registry
- B.** Chart
- C.** Kubectl
- D.** Tiller

Answer: D

Explanation

Before you can deploy Helm in an RBAC-enabled AKS cluster, you need a service account and role binding for the Tiller service.

Reference:

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

NO.191 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You have a policy stating that approvals must occur within eight hours.

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

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

Explanation

Use a gate instead of an approval instead.

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

NO.192 Your company creates a new Azure DevOps team.

D18912E1457D5D1DDCBD40AB3BF70D5D

You plan to use Azure DevOps for sprint planning.

You need to visualize the flow of your work by using an agile methodology.

Which Azure DevOps component should you use?

A. Kanban boards

B. sprint planning

C. delivery plans

D. portfolio backlogs

Answer: A

Explanation

Customizing Kanban boards

To maximize a team's ability to consistently deliver high quality software, Kanban emphasize two main practices. The first, visualize the flow of work, requires you to map your team's workflow stages and configure your Kanban board to match. Your Kanban board turns your backlog into an interactive signboard, providing a visual flow of work.

Reference:

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

NO.193 You need to recommend a Docker container build strategy that meets the following requirements

* Minimizes image sizes

* Minimizes the security surface area of the final image

What should you include in the recommendation?

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

Answer: A

Explanation

Multi-stage builds are a new feature requiring Docker 17.05 or higher on the daemon and client.

Multistage builds are useful to anyone who has struggled to optimize Dockerfiles while keeping them easy to read and maintain.

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

NO.194 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You use a Git repository for applications source control.

You need to implement a pull request strategy that reduces the history volume in the master branch.

Solution: You implement a pull request strategy that uses fast-forward merges.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

No fast-forward merge - This option merges the commit history of the source branch when the pull request closes and creates a merge commit in the target branch.

Reference:

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

NO.195 Your company has an Azure subscription named Subscription1. Subscription1 is associated to an Azure Active Directory tenant named contoso.com.

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

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

Answer Area**Objects**

a system-assigned managed identity

a cluster

an application registration in contoso.com

an RBAC binding

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

a system-assigned managed identity

a cluster

an application registration in contoso.com

an RBAC binding

a cluster

a system-assigned managed identity

an RBAC binding

Explanation**a cluster****a system-assigned managed identity****an RBAC binding**

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.

Identity edit

Name
[REDACTED]

User name
[REDACTED]@hotmail.com

Object ID
[REDACTED]

Step 3: a RBAC binding

Reference:

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

NO.196 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 Area

Aggregation granularity (Period):	<input type="checkbox"/> 1 minute <input checked="" type="checkbox"/> 5 minutes
Threshold value:	<input type="checkbox"/> Static <input checked="" type="checkbox"/> Dynamic
Operator:	<input type="checkbox"/> Greater than <input type="checkbox"/> Greater than or equal to <input type="checkbox"/> Less than or equal to <input checked="" type="checkbox"/> Less than

Answer:

Answer Area

Aggregation granularity (Period):	<input type="checkbox"/> 1 minute <input checked="" type="checkbox"/> 5 minutes
Threshold value:	<input type="checkbox"/> Static <input checked="" type="checkbox"/> Dynamic
Operator:	<input checked="" type="checkbox"/> Greater than <input type="checkbox"/> Greater than or equal to <input type="checkbox"/> Less than or equal to <input type="checkbox"/> Less than

Explanation

Answer Area

Aggregation granularity (Period):	<input type="text" value="5 minutes"/>
Threshold value:	<input type="text" value="Static"/>
Operator:	<input type="text" value="Greater than"/>

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>

NO.197 You have a private project in Azure DevOps.

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

To which security group should you add the project manager?

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

Answer: D

Explanation

Contributors have permissions to contribute fully to the project code base and work item tracking.

The main permissions they don't have or those that manage or administer resources.

Reference:

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

<https://docs.microsoft.com/en-us/azure/devops/organizations/security/permissions-access-work-tracking?view=a>

NO.198 You have multi-tier application that has an Azure Web Apps front end and an Azure SQL Database back end.

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

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

What should you include in the recommendation?

- A.** Azure Application Insights
- B.** Azure SQL Database Intelligent Insights
- C.** Azure Event Hubs
- D.** Azure Log Analytics

Answer: A

Explanation

Azure Platform as a Service (PaaS) resources, like Azure SQL and Web Sites (Web Apps), can emit performance metrics data natively to Log Analytics.

The Premium plan will retain up to 12 months of data, giving you an excellent baseline ability.

There are two options available in the Azure portal for analyzing data stored in Log Analytics and for creating queries for ad hoc analysis.

References: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-azurepass-posh>

NO.199 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: A E

Explanation

<https://github.com/microsoft/azure-pipelines-image-generation/blob/d80f81d6c98f8ce2c74b034309bb774ea8d31>

<https://github.com/actions/virtual-environments/blob/master/images/win/Windows2016-Readme.md>

NO.200 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.

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

Answer:

Source code:	Azure Repos
A common library used by multiple applications:	Azure Artifacts
Logs from automated tests and builds:	Azure Pipelines
Large and frequently updated binary assets:	Azure Storage

Explanation

Source code:

Azure Repos

A common library used by multiple applications:

Azure Artifacts

Logs from automated tests and builds:

Azure Pipelines

Large and frequently updated binary assets:

Azure Storage

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>

NO.201 You have a private project in Azure DevOps and two users named User1 and User2.

You need to add User1 and User2 to groups to meet the following requirements:

- * User1 must be able to create a code wiki.
- * User2 must be able to edit wiki pages.
- * The solution must use the principle of least privilege.

To which group should you add each user? To answer, drag the appropriate groups to the correct users. Each group 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.

Groups

Build Administrators
Contributors
Project Administrators
Project Valid Users
Stakeholders

Answer Area

User1:

User2:

Answer:

Groups

Build Administrators
Contributors
Project Administrators
Project Valid Users
Stakeholders

Answer Area

User1:

Project Administrators

User2:

Contributors

Explanation

User1: Project Administrators

User2: Contributors

User1: Project Administrators

You must have the permission Create Repository to publish code as wiki. By default, this permission is set for members of the Project Administrators group.

User2: Contributors

Anyone who is a member of the Contributors security group can add or edit wiki pages.

Anyone with access to the team project, including stakeholders, can view the wiki.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/project/wiki/wiki-create-repo>

NO.202 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?

D18912E1457D5D1DDCBD40AB3BF70D5D

A. branch policies of the master branch

B. Services in Project Settings

C. Deployment pools in Project Settings

D. branch security of the master branch

Answer: A

Explanation

Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.

Reference:

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

NO.203 You need to create and configure an Azure Storage account named az400lod11566895stor in a resource group named RG1lod11566895 to store the boot diagnostics for a virtual machine named VM1.

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

Answer:

See solution below.

Explanation

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

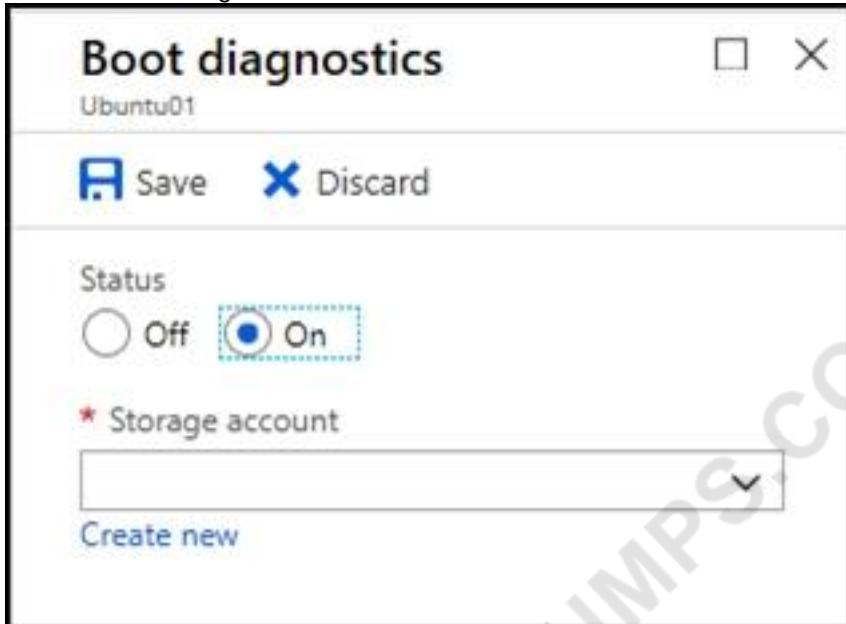
* On the Azure portal menu, select All services. In the list of resources, type Storage Accounts. As you begin typing, the list filters based on your input. Select Storage Accounts.

- * 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.

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>

NO.204 Your company uses Azure DevOps.

Only users who have accounts in Azure Active Directory can access the Azure DevOps environment.

You need to ensure that only devices that are connected to the on-premises network can access the Azure DevOps environment.

What should you do?

- A. Assign the Stakeholder access level to all users.
- B. In Azure Active Directory, configure risky sign-ins.
- C. In Azure DevOps, configure Security in Project Settings.
- D. In Azure Active Directory, configure conditional access.

Answer: D

Explanation

Conditional Access is a capability of Azure Active Directory. With Conditional Access, you can implement automated access control decisions for accessing your cloud apps that are based on

conditions.

Conditional Access policies are enforced after the first-factor authentication has been completed.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

NO.205 You need to configure an Azure web app named az400-9940427-main to contain an environmental variable named "MAX_ITEMS". The environmental variable must have a value of 50. To complete this task, sign in to the Microsoft Azure portal.

Answer:

See solution below.

Explanation

1. In the Azure portal, navigate to the az400-9940427-main app's management page. In the app's left menu, click Configuration > Application settings.

Name	Value	Type	deployment...
(no application settings to display)			

Name	Type	deployment...
(no connection strings to display)		

2. Click New Application settings

3. Enter the following:

- * Name: MAX_ITEMS
- * Value: 50

References:

<https://docs.microsoft.com/en-us/azure/app-service/configure-common>

NO.206 Your company uses Azure DevOps for the build pipelines and deployment pipelines of Java based projects.

You need to recommend a strategy for managing technical debt.

Which two actions should you include in the recommendation? Each correct answer presents part of the solution
NOTE: Each correct selection is worth one point.

- A.** Integrate Azure DevOps and SonarQube.

- B.** Integrates Azure DevOps and Azure DevTest Labs.
- C.** Configure post-deployment approvals in the deployment pipeline.
- D.** Configure pre-deployment approvals in the deployment pipeline.

Answer: A C

NO.207 You have an Azure Kubernetes Service (AKS) implementation that is RBAC-enabled. You plan to use Azure Container Instances as a hosted development environment to run containers in the AKS implementation.

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

Which three actions should you perform in sequence?

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

Actions

Run helm init.

Run az aks install-connector.

Create a YAML file.

Run az role assignment create

Run kubectl apply.

Answer Area



Answer Area

Create a YAML file.

Run kubectl apply.



Run helm init.



Answer:

Actions

Run helm init.

Run az aks install-connector.

Create a YAML file.

Run az role assignment create

Run kubectl apply.

Explanation

Create a YAML file.

Run `kubectl apply`.

Run `helm init`.

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>

NO.208 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 use Azure Pipelines to build and test a React js application.

You have a pipeline that has a single job.

You discover that installing JavaScript packages from npm takes approximately five minutes each time you run the pipeline.

You need to recommend a solution to reduce the pipeline execution time.

Solution: You recommend enabling parallel jobs for the pipeline.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead enable pipeline caching.

Note:

npm-cache is a command line utility that caches dependencies installed via npm, bower, jspm and composer.

It is useful for build processes that run [npm|bower|composer|jspm] install every time as part of their build process. Since dependencies don't change often, this often means slower build times. npm-cache helps alleviate this problem by caching previously installed dependencies on the build machine.

Reference:

<https://www.npmjs.com/package/npm-cache>

NO.209 You have an Azure DevOps organization named Contoso and an Azure subscription. You use Azure DevOps to build and deploy a web app named App1. Azure Monitor is configured to generate an email notification in response to alerts generated whenever App1 generates a server-side error.

You need to receive notifications in Microsoft Teams whenever an Azure Monitor alert is generated. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.** Create an Azure logic app that has an HTTP request trigger.
- B.** Modify the Diagnostics settings in Azure Monitor.
- C.** Modify an action group in Azure Monitor.
- D.** Create an Azure Monitor workbook.
- E.** Create an Azure logic app that has an Azure DevOps trigger.

Answer: A B

Explanation

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups-logic-app>

NO.210 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 Monitor alert that has a dynamic threshold
- B.** an Azure Automation runbook
- C.** an Azure Monitor alert that uses an action group that has an email action
- D.** the Azure Monitor autoscale settings
- E.** an Azure Monitor alert that has a static threshold

Answer: B C

NO.211 You have an Azure DevOps project that contains a release pipeline and a Git repository.

When a new code revision is committed to the repository, a build and release is triggered.

You need to ensure that release information for the pipeline is added automatically to the work items associated to the Git commit.

What should you do?

- A.** Modify the Integrations options for the pipeline.
- B.** Modify the post-deployment conditions for the last stage of the pipeline.
- C.** Add an agentless job to the pipeline.
- D.** Modify the service hooks for the project.

Answer: B

Explanation

Configure your release definition to post deployment information to Work items.

1. Open Pipelines>Releases, choose to edit your release pipeline, then choose Options>Integrations.

All pipelines > My Release

Pipeline Tasks Variables Retention Options History

General Integrations

- Report deployment status to the repository host ⓘ
- Report deployment status to Work ⓘ
- Report deployment status to Boards ⓘ
- Report deployment status to Jira ⓘ
- Enable the deployment status badge ⓘ

Reference:

<https://docs.microsoft.com/en-us/azure/devops/boards/work-items/work-item-deployments-control>

NO.212 You need to increase the security of your team's development process.

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

Security Tools

Penetration testing

Static code analysis

Threat modeling

Answer Area

Pull request:

Continuous integration:

Continuous delivery:

Answer:

Security Tools**Answer Area**

Penetration testing

Pull request: Static code analysis

Static code analysis

Continuous integration: Static code analysis

Threat modeling

Continuous delivery: Penetration testing

Explanation

<https://docs.microsoft.com/en-us/azure/devops/migrate/security-validation-cicd-pipeline?view=azure-devops&vi> So:

PR: Static Code Analysis

CI: Static Code Analysis

CD: PenTest

NO.213 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.

Build agent:

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

Release agent:

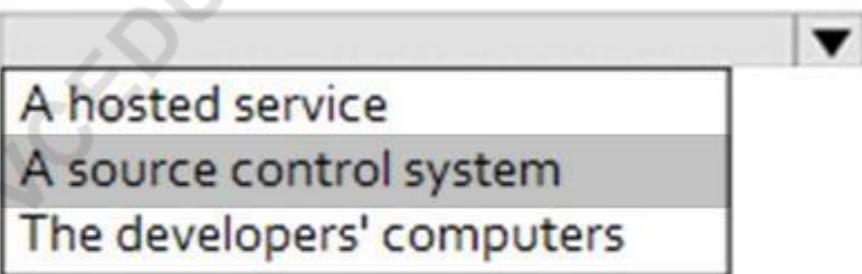
- A hosted service
- A source control system
- The developers' computers

Answer:

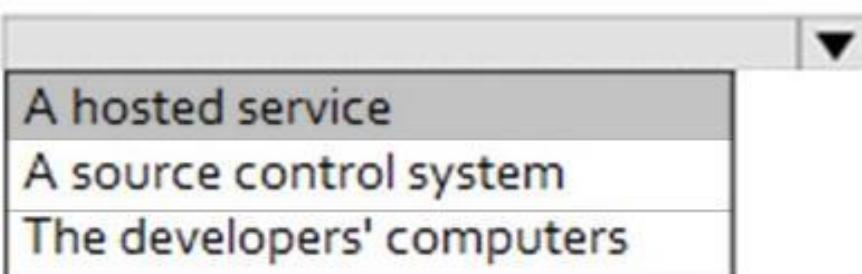
Actions	Answer Area
Create a fork	Create a repository
Create a branch	Create a branch
Add a build validation policy.	Add a build validation policy.
Add a build policy	Add a build validation policy.
Create a repository	
Add an application access policy.	

Explanation

Build agent:



Release agent:



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>

NO.214 Your company is building a new solution in Java.

The company currently uses a SonarQube server to analyze the code of .NET solutions.

You need to analyze and monitor the code quality of the Java solution.

Which task types should you add to the build pipeline?

- A.** Chef
- B.** Gradle
- C.** Octopus
- D.** Gulp

Answer: B

Explanation

SonarQube is a set of static analyzers that can be used to identify areas of improvement in your code. It allows you to analyze the technical debt in your project and keep track of it in the future. With Maven and Gradle build tasks, you can run SonarQube analysis with minimal setup in a new or existing Azure DevOps Services build task.

References:

<https://docs.microsoft.com/en-us/azure/devops/java/sonarqube?view=azure-devops>

NO.215 You manage the Git repository for a large enterprise application.

You need to minimize the data size of the repository.

How should you complete the commands? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

git gc	<input type="checkbox"/> --aggressive <input type="checkbox"/> --auto <input type="checkbox"/> --force <input type="checkbox"/> --no-prune	now
git	<input type="checkbox"/> merge <input type="checkbox"/> prune <input type="checkbox"/> rebase <input type="checkbox"/> reset	--expire now

Answer:

Answer Area

git gc	<input checked="" type="checkbox"/> --aggressive <input type="checkbox"/> --auto <input type="checkbox"/> --force <input type="checkbox"/> --no-prune	now
git	<input checked="" type="checkbox"/> merge <input checked="" type="checkbox"/> prune <input type="checkbox"/> rebase <input type="checkbox"/> reset	--expire now

Explanation

Answer Area

git gc	--aggressive
git	<input type="checkbox"/> prune <input type="checkbox"/> --expire now

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>

NO.216 You are planning projects for three customers. Each customer's preferred process for work items is shown in the following table.

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

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

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

NOTE: Each correct selection is worth one point.

Processes

Agile

CMMI

Scrum

XP

Answer Area

Litware

Contoso:

A. Datum:

Answer:

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

Explanation

Litware

Scrum

Contoso:

Agile

A. Datum:

CMMI

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.

NO.217 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.

You need to recommend changes to reduce the accumulated technical debt.

Solution: You recommend increasing the code duplication.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead reduce the code complexity.

Reference:

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

NO.218 You use Azure Pipelines to manage the build and deployment of apps.

You are planning the release strategies for a new app. You need to choose strategies for the following scenarios:

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

Answer Area

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

Progressive exposure
Blue/green
Feature flags

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

Progressive exposure
Blue/green
Feature flags

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

Progressive exposure
Blue/green
Feature flags

Answer:

Answer Area

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

Progressive exposure
Blue/green
Feature flags

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

Progressive exposure
Blue/green
Feature flags

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

Progressive exposure
Blue/green
Feature flags

Explanation

Answer Area

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

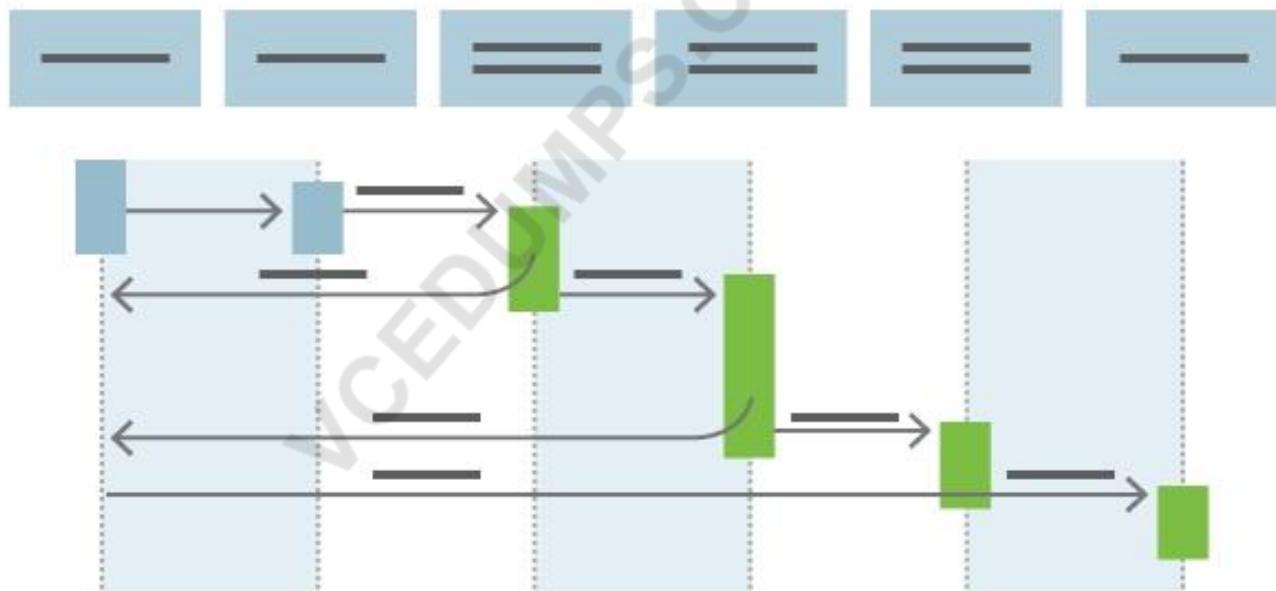
Code will be deployed to enable functionality that will be available in later releases of the app:

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

Box 1: Progressive exposure

Continuous Delivery may sequence multiple deployment "rings" for progressive exposure (also known as

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

**Box 2: Feature flags**

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

Box 3: Blue/green

Blue/green deployments which means that instead of replacing the previous version (here we refer to this version as blue), we bring up the new version (here referred to as the green version) next to the existing version, but not expose it to the actual users right away. On the condition of having successfully validated that the green version works correctly, we will promote this version to the public version by changing the routing configuration without downtime. If something is wrong with the green version we can revert back without users every noticing interruptions.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/learn/what-is-continuous-delivery>

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

<https://medium.com/@denniszielke/continuous-kubernetes-blue-green-deployments-on-azure-using-nginx-appga>

NO.219 Your company has 60 developers who are assigned to four teams. Each team has 15 members.

The company uses an agile development methodology.

You need to structure the work of the development teams so that each team owns their respective work while working together to reach a common goal.

Which parts of the taxonomy should you enable the team to perform autonomously?

- A.** Features and Tasks
- B.** Initiatives and Epics
- C.** Epics and Features
- D.** Stories and Tasks

Answer: A

Explanation

A feature typically represents a shippable component of software.

Features, examples:

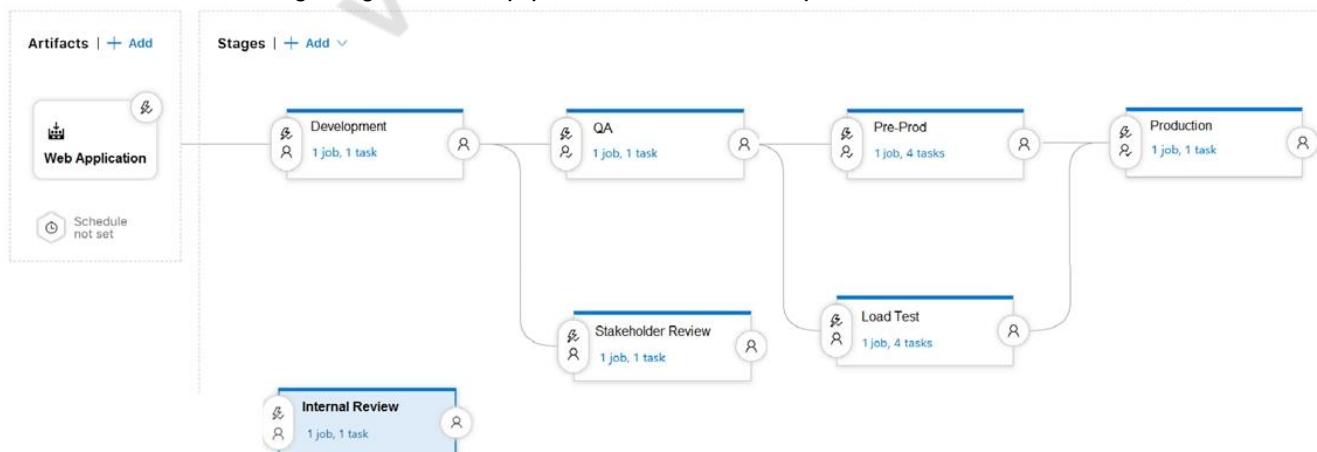
- * Add view options to the new work hub
- * Add mobile shopping cart
- * Support text alerts
- * Refresh the web portal with new look and feel

User Stories and Tasks are used to track work. Teams can choose how they track bugs, either as requirements or as tasks Reference:

<https://docs.microsoft.com/en-us/azure/devops/boards/backlogs/define-features-epics>

<https://docs.microsoft.com/en-us/azure/devops/boards/work-items/about-work-items>

NO.220 You are configuring a release pipeline in Azure DevOps as shown in the exhibit.



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

NOTE: Each correct selection is worth one point.

How many stages have triggers set?

0
1
2
3
4
5
6
7

Which component should you modify to enable continuous delivery?

The Development stage
The Internal Review stage
The Production stage
The Web Application artifact

Answer:

How many stages have triggers set?

0
1
2
3
4
5
6
7

Which component should you modify to enable continuous delivery?

The Development stage
The Internal Review stage
The Production stage
The Web Application artifact

Explanation

How many stages have triggers set?

0
1
2
3
4
5
6
7

Which component should you modify to enable continuous delivery?

The Development stage
The Internal Review stage
The Production stage
The Web Application artifact

Box 1: 5

There are five stages: Development, QA, Pre-production, Load Test and Production. They all have triggers.

Box 2: The Internal Review stage

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

NO.221 You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 and an Azure Standard Load Balancer named LB1.

LB1 distributes incoming requests across VMSS1 instances.

You use Azure DevOps to build a web app named App1 and deploy App1 to VMSS1. App1 is accessible via HTTPS only and configured to require mutual authentication by using a client certificate.

You need to recommend a solution for implementing a health check of App1. The solution must meet the following requirements:

- * Identify whether individual instances of VMSS1 are eligible for an upgrade operation.
- * Minimize administrative effort.

What should you include in the recommendation?

- A.** the Custom Script Extension
- B.** the Application Health extension
- C.** Azure Monitor autoscale
- D.** an Azure Load Balancer health probe

Answer: D

NO.222 You have a private GitHub repository.

You need to display the commit status of the repository on Azure Boards.

What should you do first?

- A.** Create a GitHub action in GitHub.
- B.** Add the Azure Pipelines app to the GitHub repository.
- C.** Configure multi-factor authentication (MFA) for your GitHub account.
- D.** Add the Azure Boards app to the repository.

Answer: D

Explanation

To connect Azure Boards to GitHub.com, connect and configure from Azure Boards. Or, alternatively, install and configure the Azure Boards app from GitHub. Both methods have been streamlined and support authenticating and operating via the app rather than an individual.

Note (see step 4 below):

Add a GitHub connection:

- * Sign into Azure Boards.
- * Choose (1) Project Settings, choose (2) GitHub connections and then (3) Connect your GitHub account.
 - * If this is your first time connecting to GitHub from Azure Boards, you will be asked to sign in using your GitHub credentials. Choose an account for which you are an administrator for the repositories you want to connect to.
 - * The Add GitHub Repositories dialog automatically displays and selects all GitHub.com repositories for which you are an administrator. Unselect any repositories that you don't want to participate in the integration.

Add GitHub repositories

Add the GitHub repositories you want to use with your Azure Boards.

Filter by keywords

Viewing 4, 4 selected

- JamalHart/fabrikam-apps-2
- JamalHart/fabrikam-demo
- JamalHart/fabrikam-open-source
- JamalHart/fabrikam-suite

Save

Reference:

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

NO.223 You have an Azure function hosted in an App Service plan named az400-9940427-func1. You need to configure az400-9940427-func1 to upgrade the functions automatically whenever new code is committed to the master branch of <https://github.com/Azure-Samples/functions-quickstart>. To complete this task, sign in to the Microsoft Azure portal.

Answer:

See solution below.

Explanation

1. Open Microsoft Azure Portal
2. Log into your Azure account, select App Services in the Azure portal left navigation, and then select az400-9940427-func1.
3. On the app page, select Deployment Center in the left menu.
4. On the Build provider page, select Azure Pipelines (Preview), and then select Continue.
5. On the Configure page, in the Code section:
For GitHub, drop down and select the Organization, Repository, and Branch you want to deploy continuously.

6. Select Continue.
7. On the Test page, choose whether to enable load tests, and then select Continue.
8. Depending on your App Service plan pricing tier, you may see a Deploy to staging page. Choose whether to enable deployment slots, and then select Continue.
9. After you configure the build provider, review the settings on the Summary page, and then select Finish.

References:

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

NO.224 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: D

Explanation

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

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

Credential managers let you use the same credentials that you use for the Azure DevOps Services web portal. Credential managers support multi-factor authentication through Microsoft account or Azure Active Directory (Azure AD). Besides supporting multi-factor authentication with Azure Repos, credential managers also support two-factor authentication with GitHub repositories.

Reference:

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

NO.225 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

Explanation

To deploy your solution, you can use either a single template or a main template with many related templates.

The related template can be either a separate file that is linked to from the main template, or a template that is nested within the main template.

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

NO.226 You are developing an application. The application source has multiple branches.

You make several changes to a branch used for experimentation.

You need to update the main branch to capture the changes made to the experimentation branch and override the history of the Git repository.

Which Git option should you use?

- A.** Rebase
- B.** Fetch
- C.** Merge
- D.** Push

Answer: C

Explanation

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

NO.227 Which package feed access levels should be assigned to the Developers and Team Leaders groups for the investment planning applications suite? To answer, drag the appropriate access levels to the correct groups.

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

NOTE: Each correct selection is worth one point.

Access Levels

Answer Area

Collaborator

Developers:

Contributor

Team Leaders:

Owner

Reader

Answer:

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

Explanation

Developers:

Reader

Team Leaders:

Owner

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				✓

NO.228 You plan to deploy a website that will be hosted in two Azure regions.

You need to create an Azure Traffic Manager profile named az40011566895n1-tm in a resource group named RG1lod11566895. The solution must ensure that users will always connect to a copy of the website that is in the same country.

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

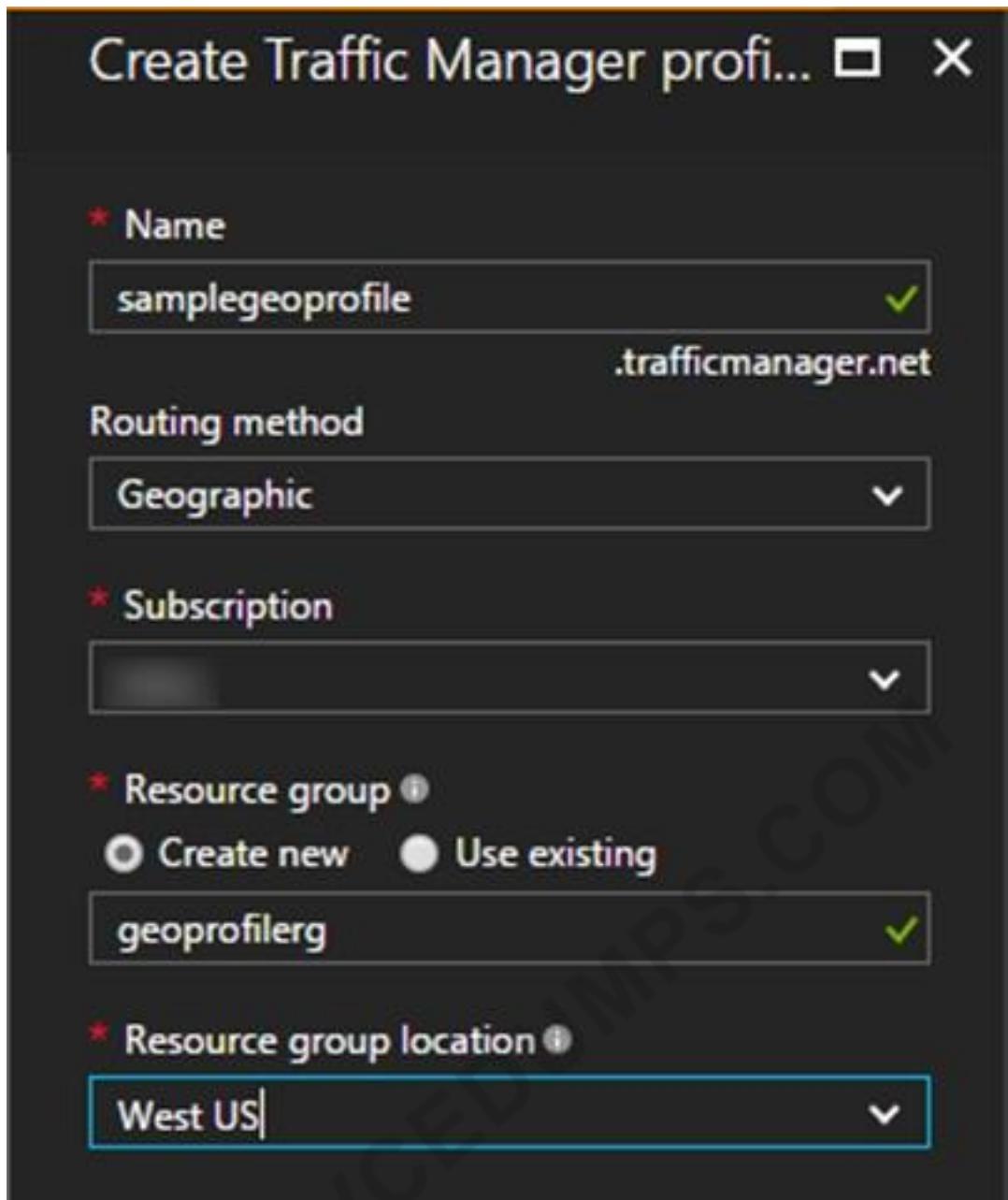
Answer:

See solution below.

Explanation

1. Go to the Azure portal, navigate to Traffic Manager profiles and click on the Add button to create a routing profile.

2. In the Create Traffic Manager profile, enter, or select these settings: Name: az40011566895n1-tm, Routing method: Geographic, Resource group: RG1lod11566895



Note: Traffic Manager profiles can be configured to use the Geographic routing method so that users are directed to specific endpoints (Azure, External or Nested) based on which geographic location their DNS query originates from. This empowers Traffic Manager customers to enable scenarios where knowing a user's geographic region and routing them based on that is important.

Reference:

<https://azure.microsoft.com/en-us/blog/announcing-the-general-availability-of-geographic-routing-capability-in-a/>

NO.229 You have a brand policy in a project in Azure DevOps. The policy requires that code always builds successfully.

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

What should you do?

- A. From the Security setting of the repository, modify the access control for the user.
- B. From the Security settings of the branch, modify the access control for the user.

- C.** Add the user to the Build Administrators group,
D. Add the user to the Project Administrators group

Answer: B

Explanation

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

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

NO.230 You are configuring Azure DevOps build pipelines.

You plan to use hosted build agents.

Which build agent pool should you use to compile each application type? To answer, drag the appropriate build agent pools to the correct application types. Each build agent pool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Build Agent Pools

Answer Area

Hosted Windows Container

An application that runs on iOS:

Hosted Ubuntu 1604

An Internet Information Services (IIS) web application
that runs in Docker:

Hosted macOS

Hosted

Default

Answer:

Build Agent Pools

Answer Area

Hosted Windows Container

An application that runs on iOS:

Hosted Ubuntu 1604

Hosted macOS

Hosted macOS

Hosted

Hosted

Default

Explanation

An application that runs on iOS:	Hosted macOS
An Internet Information Services (IIS) web application that runs in Docker:	Hosted

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.

NO.231 To resolve the current technical issue, what should you do to the Register-AzureRmAutomationDscNode command?

- A. Change the value of the ConfigurationMode parameter.
- B. Replace the Register-AzureRmAutomationDscNode cmdlet with Register-AzureRmAutomationScheduledRunbook
- C. Add the AllowModuleOverwrite parameter.
- D. Add the DefaultProfile parameter.

Answer: A

Explanation

Change the ConfigurationMode parameter from ApplyOnly to ApplyAndAutocorrect.

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

Scenario: Current Technical Issue

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

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

Register-AzureRmAutomationDscNode

```
-ResourceGroupName 'TestResourceGroup'
-AutomationAccountName 'LitwareAutomationAccount'
-AzureVMName $vmaname
-ConfigurationMode 'ApplyOnly'
```

References:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode?vi>

NO.232 You configure an Azure Application Insights availability test.

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

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

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

- A. an ApiConnection trigger

- B.** a Request trigger
C. an HTTPWebhook trigger
D. an HTTP trigger

Answer: C

Explanation

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

Reference:

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

NO.233 Your company uses Azure DevOps for Git source control.

You have a project in Azure DevOps named Contoso App that contains the following repositories:

- * <https://dev.azure.com/contoso/contoso-app/core-api>
- * <https://dev.azure.com/contoso/contoso-app/core-spa>
- * <https://dev.azure.com/contoso/contoso-app/core-db>

You need to ensure that developers receive Slack notifications when there are pull requests created for Contoso App.

What should you run in Slack? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

/azrepos	<input type="checkbox"/> feedback <input type="checkbox"/> signin <input checked="" type="checkbox"/> subscribe <input type="checkbox"/> subscriptions	<input type="checkbox"/> https://dev.azure.com/contoso/contoso-app <input type="checkbox"/> https://dev.azure.com/contoso/contoso-app/core-api <input type="checkbox"/> https://dev.azure.com/contoso/contoso-app/core-db <input type="checkbox"/> https://dev.azure.com/contoso/contoso-app/core-spa
----------	---	--

Answer:

/azrepos	<input type="checkbox"/> feedback <input checked="" type="checkbox"/> signin <input checked="" type="checkbox"/> subscribe <input type="checkbox"/> subscriptions	<input type="checkbox"/> https://dev.azure.com/contoso/contoso-app <input type="checkbox"/> https://dev.azure.com/contoso/contoso-app/core-api <input type="checkbox"/> https://dev.azure.com/contoso/contoso-app/core-db <input type="checkbox"/> https://dev.azure.com/contoso/contoso-app/core-spa
----------	--	--

Explanation

/azrepos	<input type="checkbox"/> feedback <input type="checkbox"/> signin <input checked="" type="checkbox"/> subscribe <input type="checkbox"/> subscriptions	<input type="checkbox"/> https://dev.azure.com/contoso/contoso-app <input type="checkbox"/> https://dev.azure.com/contoso/contoso-app/core-api <input type="checkbox"/> https://dev.azure.com/contoso/contoso-app/core-db <input type="checkbox"/> https://dev.azure.com/contoso/contoso-app/core-spa
----------	---	--

Box 1: subscribe

To start monitoring all Git repositories in a project, use the following slash command inside a channel:

/azrepos subscribe [project url]

Box 2: <https://dev.azure.com/contoso/contoso-app>

You can also monitor a specific repository using the following command:

/azrepos subscribe [repository url]

The repository URL can be to any page within your repository that has your repository name.

For example, for Git repositories, use:

/azrepos subscribe https://dev.azure.com/myorg/myproject/_git/myrepository Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/integrations/repos-slack>

NO.234 Your company deploys applications in Docker containers.

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

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

What should you configure?

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

Answer: C

Explanation

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

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

References:

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

NO.235 You have the following Azure policy.

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

You assign the policy to the Tenant root group.

What is the effect of the policy?

- A. prevents all http traffic to existing Azure Storage accounts

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

Answer: B

Explanation

Denies non HTTPS traffic.

NO.236 Your company is creating a suite of three mobile applications.

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

NOTE: Each correct selection is worth one point.

Groups to control the build access:

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

Group type:

Private
Public
Shared

Answer:

Groups to control the build access:

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

Group type:

Private
Public
Shared

Explanation

Groups to control the build access:



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. Examples 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>

NO.237 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You plan to update the Azure DevOps strategy of your company.

You need to identify the following issues as they occur during the company's development process:

- * Licensing violations
- * Prohibited libraries

Solution: You implement continuous deployment.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Instead implement continuous integration.

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

WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against

WhiteSource constantly-updated definitive database of open source repositories.

Reference:

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

NO.238 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

Delete and recreate the repository.

Add Config.json to the .gitignore file.

Run the git add .gitignore command.

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

NO.239 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.

Convert the .docx files to:

LaTeX Typesetting (.tex)
Markdown (.md)
Portable Document Format (.pdf)

Convert the flow charts to:

Mermaid graph diagrams (.md)
Portable Network Graphics (.png)
Tagged Image File Format (.tiff)

Answer:

Convert the .docx files to:

LaTeX Typesetting (.tex)
Markdown (.md)
Portable Document Format (.pdf)

Convert the flow charts to:

Mermaid graph diagrams (.md)
Portable Network Graphics (.png)
Tagged Image File Format (.tiff)

NO.240 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

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

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

You need to recommend a solution to deploy the resources.

Solution: Create a main template that will deploy the resources in one resource group and a nested template that will deploy the resources in the other resource group.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Use two linked templates, instead of the nested template.

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

NO.241 You have an Azure Kubernetes Service (AKS) pod.

You need to configure a probe to perform the following actions:

- * Confirm that the pod is responding to service requests.
- * Check the status of the pod four times a minute.
- * Initiate a shutdown if the pod is unresponsive.

How should you complete the YAML configuration file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
apiVersion: v1
kind: Pod
metadata:
  labels:
    test: readiness-and-liveness
  name: readiness-http
spec:
  containers:
    - name: container1
      image: k8s.gcr.io/readiness-and-liveness
      args:
        - /server
      livenessProbe:
        httpGet:
          path: /checknow
          port: 8123
          httpHeaders:
            - name: Custom-Header
              value: CheckNow
      readinessProbe:
        initialDelaySeconds: 15
        periodSeconds: 15
        timeoutSeconds: 15
      shutdownProbe:
```

Answer:

Answer Area

```
apiVersion: v1
kind: Pod
metadata:
  labels:
    test: readiness-and-liveness
  name: readiness-http
spec:
  containers:
    - name: container1
      image: k8s.gcr.io/readiness-and-liveness
      args:
        - /server
      livenessProbe:
        httpGet:
          path: /checknow
          port: 8123
          httpHeaders:
            - name: Custom-Header
              value: CheckNow
      readinessProbe:
        httpGet:
          path: /checknow
          port: 8123
          httpHeaders:
            - name: Custom-Header
              value: CheckNow
      shutdownProbe:
        httpGet:
          path: /checknow
          port: 8123
          httpHeaders:
            - name: Custom-Header
              value: CheckNow
      startupProbe:
        httpGet:
          path: /checknow
          port: 8123
          httpHeaders:
            - name: Custom-Header
              value: CheckNow
      initialDelaySeconds: 15
      periodSeconds: 15
      timeoutSeconds: 15
```

Explanation

```

spec:
  containers:
    - name: container1
      image: k8s.gcr.io/readiness-and-liveness
      args:
        - /server

      livenessProbe:
      readinessProbe:
      ShutdownProbe:
      startupProbe:

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

      initialDelaySeconds: 15
      periodSeconds: 15
      timeoutSeconds: 15

```

Box 1: readinessProbe:

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

Reference:

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

NO.242 Your company develops an app for OS. All users of the app have devices that are members of a private distribution group in Microsoft Visual Studio App Center.

You plan to distribute a new release of the app.

You need to identify which certificate file you require to distribute the new release from App Center. Which file type should you upload to App Center?

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

Answer: D

Explanation

A successful iOS device build will produce an ipa file. In order to install the build on a device, it needs to be signed with a valid provisioning profile and certificate. To sign the builds produced from a

branch, enable code signing in the configuration pane and upload a provisioning profile (.mobileprovision) and a valid certificate (.p12), along with the password for the certificate.

References:

<https://docs.microsoft.com/en-us/appcenter/build/xamarin/ios/>

NO.243 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: C

Explanation

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

Reference:

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

NO.244 You have an Azure DevOps organization named Contoso, an Azure DevOps project named Project1, an Azure subscription named Sub1, and an Azure key vault named vault1.

You need to ensure that you can reference the values of the secrets stored in vault1 in all the pipelines of Project1. The solution must prevent the values from being stored in the pipelines.

What should you do?

- A. Create a variable group in Project1.
- B. Add a secure file to Project1.
- C. Modify the security settings of the pipelines.
- D. Configure the security policy of Contoso.

Answer: A

Explanation

Use a variable group to store values that you want to control and make available across multiple pipelines.

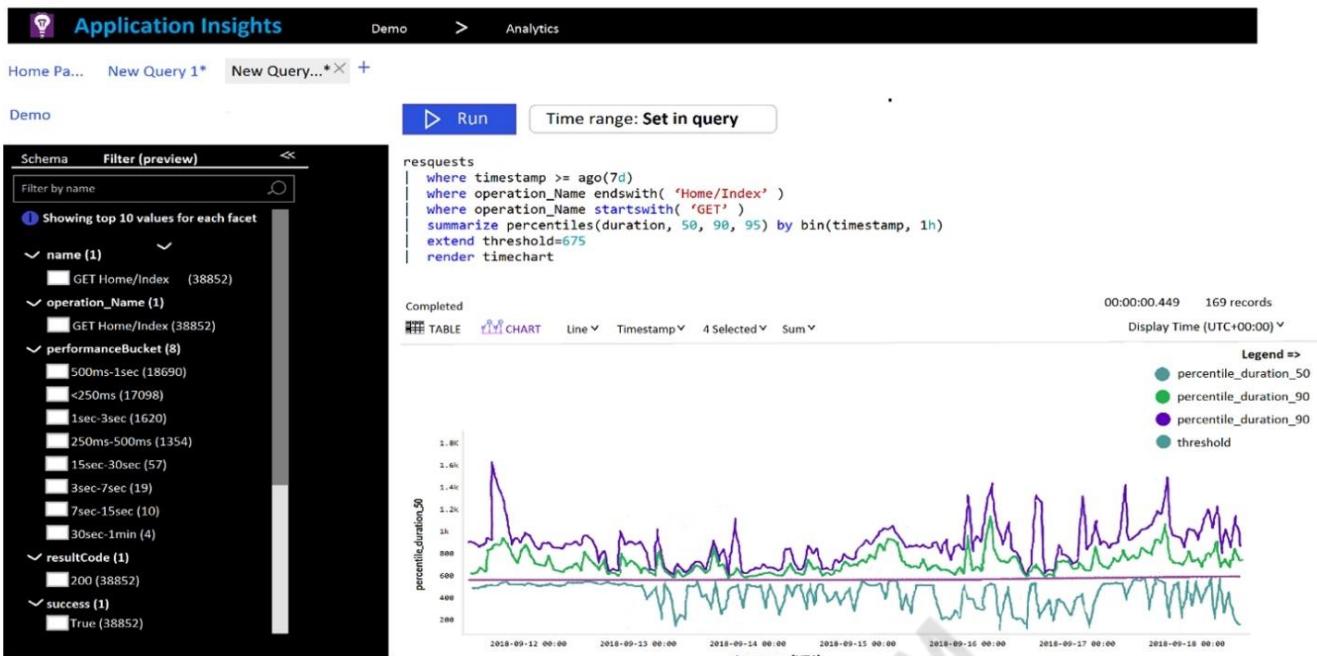
References:

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

<https://docs.microsoft.com/en-us/azure/devops/pipelines/library/variable-groups?view=azure-devops&tabs=yaml>

NO.245 You plan to create alerts that will be triggered based on the page load performance of a home page.

You have the Application Insights log query shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

To create an alert based on the page load experience of most users, the alerting level must be based on [answer choice].

percentile.duration_50
percentile.duration_90
percentile.duration_95
threshold

To only create an alert when authentication error occurs on the server, the query must be filtered on [answer choice].

item Type
resultCode
source
success

Answer:

To create an alert based on the page load experience of most users, the alerting level must be based on [answer choice].

percentile.duration_50
percentile.duration_90
percentile.duration_95
threshold

To only create an alert when authentication error occurs on the server, the query must be filtered on [answer choice].

item Type
resultCode
source
success

Explanation

To create an alert based on the page load experience of most users, the alerting level must be based on [answer choice].

percentile_duration_50
percentile_duration_90
percentile_duration_95
threshold

To only create an alert when authentication error occurs on the server, the query must be filtered on [answer choice].

item Type
resultCode
source
success

Box 1: percentile_duration_95

Box 2: success

For example -

requests

```
| project name, url, success
| where success == "False"
```

This will return all the failed requests in my App Insights within the specified time range.

Reference:

<https://devblogs.microsoft.com/premier-developer/alerts-based-on-analytics-query-using-custom-log-search/>

NO.246 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

Explanation

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

Reference:

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

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v2-aspnet-webapp>

NO.247 How should you configure the release retention policy for the investment planning depletions suite? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Required secrets:

Certificate
Personal access token
Shared Access Authorization token
Username and password

Storage location:

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

Answer:

Required secrets:

Certificate
Personal access token
Shared Access Authorization token
Username and password

Storage location:

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

Explanation

Required secrets:

Certificate
Personal access token
Shared Access Authorization token
Username and password

Storage location:

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

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>

NO.248 You have a project in Azure DevOps that uses packages from multiple public feeds. Some of the feeds are unreliable.

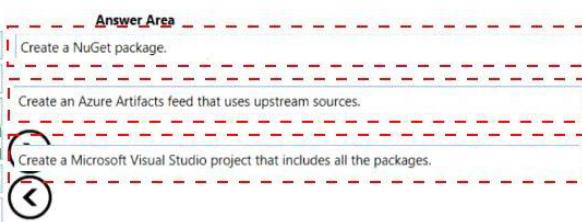
You need to consolidate the packages into a single feed.

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

- Actions**
- Create an npm package.
 - Create an Azure Artifacts feed that uses upstream sources.
 - Modify the configuration files to reference the Azure Artifacts feed.
 - Run an initial package restore.
 - Create a NuGet package.
 - Create a Microsoft Visual Studio project that includes all the packages.

Answer Area**Answer:**

- Actions**
- Create an npm package.
 - Create an Azure Artifacts feed that uses upstream sources.
 - Modify the configuration files to reference the Azure Artifacts feed.
 - Run an initial package restore.
 - Create a NuGet package.
 - Create a Microsoft Visual Studio project that includes all the packages.

**Explanation**

Create a NuGet package.

Create an Azure Artifacts feed that uses upstream sources.

Create a Microsoft Visual Studio project that includes all the packages.

Step 1: Create a NuGet package.

NuGet and Maven are public package managers that support multiple feeds.

Step 2: Create an Azure Artifacts feed that uses upstream sources

If you want to use packages from multiple feeds, use upstream sources to bring packages from multiple feeds together into a single feed.

Step 3: Create a Microsoft Visual Studio project that includes all the packages Consume NuGet packages from upstream sources: Now you can open Visual Studio and install packages from the upstream sources you just configured.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/artifacts/how-to/set-up-upstream-sources>

NO.249 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 AddressPrefixes to 10.0.0.0/24 in order to support only 256 total IP addresses.
addressSpace": {"addressPrefixes": ["10.0.0.0/24"]},
5. Change the firstSubnet addressprefix to 10.0.0.0/26 to support only 64 total IP addresses.
"subnets": [
{
"name": "firstSubnet",
"properties": {
"addressPrefix": "10.0.0.0/24"
}
}
6. Select Save.

Microsoft Azure Stack - Administration

Home > New > Custom deployment

Custom deployment Deploy from a custom template

Template

Edit template

Parameters

Edit parameters

Subscription

Default Provider Subscription

Create new **Use existing**

Resource group

Create new **Use existing**

Resource group location

local

Create

The screenshot shows the Microsoft Azure Stack Administration interface. On the left is a navigation sidebar with various links: Create a resource, All services, Favorites (Dashboard, All resources, Resource groups, Virtual machines, Recent, Plans, Offers, Monitor, Marketplace management). The main area is titled 'Custom deployment' with the sub-instruction 'Deploy from a custom template'. It contains three main sections: 'Template' (highlighted with a red box), 'Parameters', and 'Subscription'. The 'Template' section has an 'Edit template' link. The 'Parameters' section has an 'Edit parameters' link. The 'Subscription' section shows 'Default Provider Subscription' selected. Below that, under 'Resource group', 'Create new' is selected. Under 'Resource group location', 'local' is selected. At the bottom is a large blue 'Create' button.

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.

VCEDUMPS.COM

Microsoft Azure Stack - Administration

< Home > New > Custom deployment

Custom deployment
Deploy from a custom template

Template Edit template >

Parameters Edit parameters >

Subscription Default Provider Subscription

Resource group i
 Create new Use existing
test-rg

Resource group location local

Create

The screenshot shows the Microsoft Azure Stack Administration interface. On the left, there's a sidebar with various navigation options: 'Create a resource', 'All services', 'FAVORITES' (containing 'Dashboard', 'All resources', 'Resource groups', 'Virtual machines', 'Recent', 'Plans', 'Offers', 'Monitor', and 'Marketplace management'). The main area is titled 'Custom deployment' with the sub-instruction 'Deploy from a custom template'. It contains three main sections: 'Template' (with 'Edit template' link), 'Parameters' (with 'Edit parameters' link), and 'Subscription' (set to 'Default Provider Subscription'). The 'Resource group' section is expanded, showing two options: 'Create new' (radio button) and 'Use existing' (radio button, which is selected). A dropdown menu below shows 'test-rg'. This 'Resource group' section is highlighted with a red rectangular box. At the bottom right of the dialog is a large blue 'Create' button.

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>

NO.250 You need to create an instance of Azure Application Insights named az400-9940427-main and configure the instance to receive telemetry data from an Azure web app named az400-9940427-main.

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

Answer:

See solution below.

Explanation

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.

The screenshot shows the Azure Marketplace interface with a sidebar of icons on the left. At the top, there's a 'New' button, a search bar, and a close button. Below the search bar, there are sections for 'Azure Marketplace' and 'Featured'. The 'Featured' section lists several services with their icons and names: DevOps Project, DevTest Labs, Chef Automate, Application Insights (which is highlighted with a red box), API Management, Jenkins, GitHub Enterprise Server, Enterprise DC/OS on Azure, and Ansible Tower.

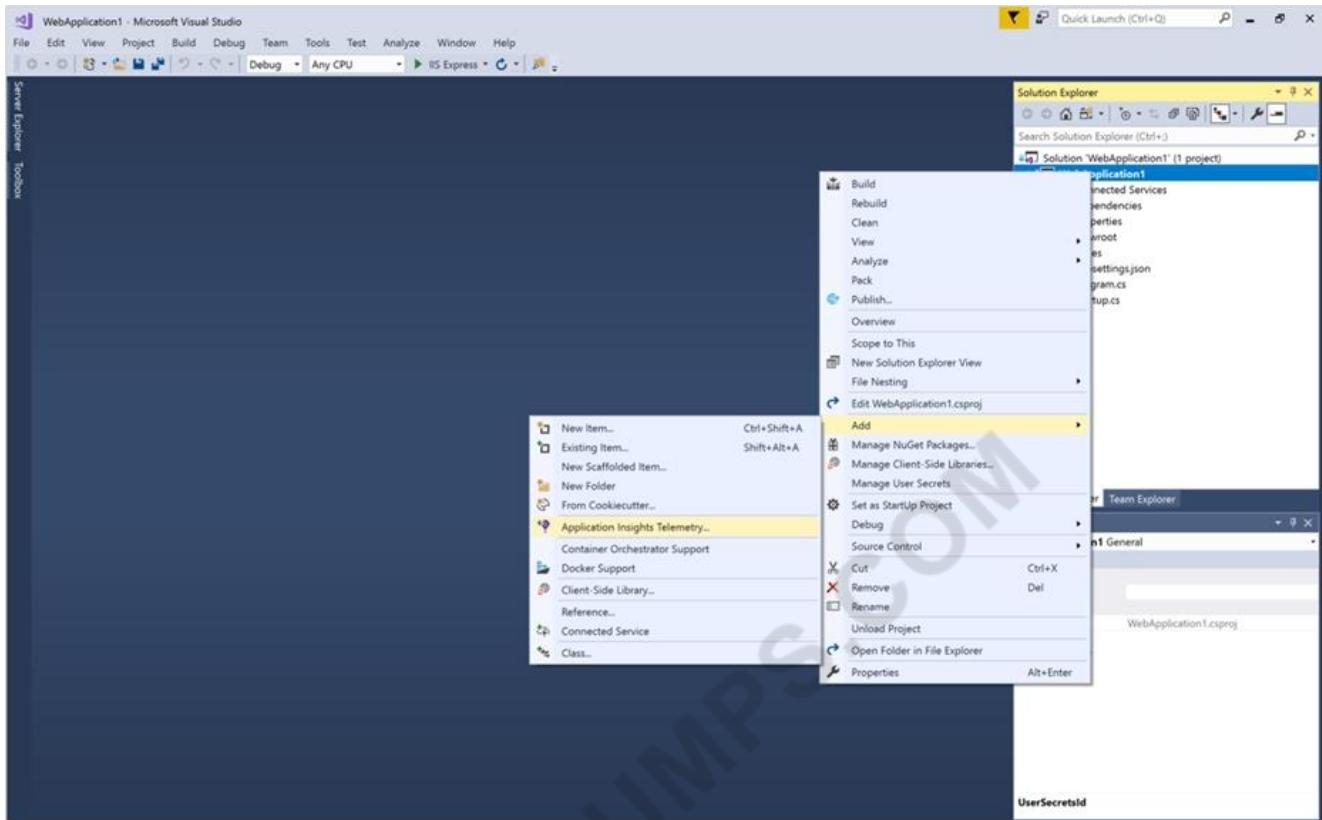
Category	Service	Description
Get started	DevOps Project	Quickstart tutorial
Recently created	DevTest Labs	Quickstart tutorial
Compute	Chef Automate	Learn more
Networking	Application Insights	Quickstart tutorial
Storage	API Management	Quickstart tutorial
Web	Jenkins	Learn more
Mobile	GitHub Enterprise Server	Learn more
Containers	Enterprise DC/OS on Azure	Learn more
Databases	Ansible Tower	Learn more
Analytics		
AI + Machine Learning		
Internet of Things		
Mixed Reality		
Integration		
Security		
Identity		
Developer Tools		
Management Tools		
Software as a Service (SaaS)		
Blockchain		

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

Name: az400-9940427-main

Step 2: Configure App Insights SDK

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



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

References:

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

NO.251 You provision an Azure Kubernetes Service (AKS) cluster that has RBAC enabled. You have a Helm chart for a client application.

You need to configure Helm and Tiller on the cluster and install the chart.

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

Commands**Answer Area**

helm install

kubectl create

helm completion

helm init

helm serve

**Answer:****Commands****Answer Area**

helm install

kubectl create

helm completion

helm init

helm serve

kubectl create

helm init

helm install

**Explanation**

```
kubectl create
```

```
helm init
```

```
helm install
```

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

NO.252 You have a project Azure DevOps.

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

The templates will reference secrets stored in Azure Key Vault.

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

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

NOTE: Each correct selection is worth one point.

```

"resources": [
{
  "apiversion": "2018-05-01",
  "name" : "secrets",
  "type": "Microsoft.KeyVault/vaults",
  "Microsoft.Resources/deployment",
  "Microsoft.Subscription/subscriptions".
"properties": {
  "mode" : "Incremental",
  "deployment"
  "template"
  "templateLink"
contentVersion" : "1.0.0.0",
  "uri" : "[uri(parameters('_artifactsLocation'),
  concat('./nested/sqlserver.json',
  parameters('_artifactsLocationSasToken')))]"
},
"parameters": {
  "secret": {
    "reference": {
      "keyVault": {
        "id": "[resourceId(parameters('vaultSubscription'),
        parameters('vaultResourceGroupName'),
        'Microsoft.KeyVault/vaults',
        parameters('vaultName'))]"
      },
      "secretName": "[parameters('secretName')]"
    }
  }
}
],

```

Answer:

```
"resources": [
  {
    "apiversion": "2018-05-01",
    "name" : "secrets",
    "type": "Microsoft.KeyVault/vaults",
    "Microsoft.Resources/deployment",
    "Microsoft.Subscription/subscriptions".
  },
  {
    "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

```
"resources": [
  {
    "apiVersion": "2018-05-01",
    "name" : "secrets",
    "type": "Microsoft.Resources/deployment",
    "Microsoft.KeyVault/vaults",
    "Microsoft.Subscription/subscriptions".
  },
  "properties": {
    "mode" : "Incremental",
    "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')]"
      }
    }
  }
},
```

NO.253 You need to ensure that Microsoft Visual Studio 2017 can remotely attach to an Azure Function named fa-11566895.

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

Answer:

See solution below.

Explanation

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.

Reference:

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

NO.254 Your company plans to use an agile approach to software development

You need to recommend an application to provide communication between members of the development team who work in locations around the world. The application must meet the following requirements:

- * Provide the ability to isolate the members of efferent project teams into separate communication channels and to keep a history of the chats within those channels.
- * Be available on Windows 10, Mac OS, iOS, and Android operating systems.
- * Provide the ability to add external contractors and suppliers to projects.
- * Integrate directly with Azure DevOps.

What should you recommend?

- A.** Octopus
- B.** Bamboo
- C.** Microsoft Project
- D.** Slack

Answer: D

Explanation

Slack is a popular team collaboration service that helps teams be more productive by keeping all communications in one place and easily searchable from virtually anywhere. All your messages, your files, and everything from Twitter, Dropbox, Google Docs, Azure DevOps, and more all together. Slack also has fully native apps for iOS and Android to give you the full functionality of Slack wherever you go.

Integrated with Azure DevOps

This integration keeps your team informed of activity happening in its Azure DevOps projects. With this integration, code check-ins, pull requests, work item updates, and build events show up directly in your team's Slack channel.

Note: Microsoft Teams would also be a correct answer, but it is not an option here.

References:

<https://marketplace.visualstudio.com/items?itemName=ms-vsts.vss-services-slack>

NO.255 You have an application named App1 that has a custom domain of app.contoso.com.

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

Create test

Basic Information

* Test name

availability



Learn more about configuring tests against applications hosted behind a firewall

Test type

URL ping test



* URL ⓘ

https://app.contoso.com



Parse dependent requests ⓘ



Enable retries for availability test failures. ⓘ



Test frequency ⓘ

5 minutes



Test locations

4 location(s) configured

Success criteria

Test Timeout ⓘ

30 seconds



Status code must equal

200



Content must contain

Copyright Contoso

▼ Alerts
Enabled

Create

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

NOTE: Each correct selection is worth one point.

The test will execute [answer choice].

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

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

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

Answer:

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

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

Box 1: every five minutes at a random location

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

Box 2:

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

Reference:

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

NO.256 You use WhiteSource Bolt to scan a Node.js application.

The WhiteSource Bolt scan identifies numerous libraries that have invalid licenses. The libraries are used only during development and are not part of a production deployment.

You need to ensure that WhiteSource Bolt only scans production dependencies.

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

NOTE: Each correct selection is worth one point.

- A. Run npm install and specify the --production flag.
- B. Modify the WhiteSource Bolt policy and set the action for the licenses used by the development tools to Reassign.
- C. Modify the devDependencies section of the project's Package.json file.
- D. Configure WhiteSource Bolt to scan the node_modules directory only.

Answer: A C

Explanation

A: To resolve NPM dependencies, you should first run "npm install" command on the relevant folders before executing the plugin.

C: All npm packages contain a file, usually in the project root, called package.json - this file holds various metadata relevant to the project. This file is used to give information to npm that allows it to identify the project as well as handle the project's dependencies. It can also contain other metadata such as a project description, the version of the project in a particular distribution, license information, even configuration data - all of which can be vital to both npm and to the end users of the package.

Reference:

<https://whitesource.atlassian.net/wiki/spaces/WD/pages/34209870/NPM+Plugin>

<https://nodejs.org/en/knowledge/getting-started/npm/what-is-the-file-package-json>

NO.257 You are building an ASP.NET Core application.

You plan to create an application utilization baseline by capturing telemetry data.

You need to add code to the application to capture the telemetry data. The solution must minimize the costs of storing the telemetry data.

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

NOTE: Each correct selection is worth one point.

- A) Add the <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 A
 - B. Option B

C. Option C

D. Option D

E. Option E

Answer: B E

NO.258 Note: This question is part of * series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You have a policy stating that approvals must occur within eight hours.

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

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

Solution: From Post-deployment conditions, you modify the Time between re-evaluation of gates option.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

Use a gate From Pre-deployment conditions instead.

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

NO.259 You are automating the build process for a Java-based application by using Azure DevOps.

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

What should you use?

A. Cobertura

B. Bullseye Coverage

C. MSTest

D. Coverlet

Answer: A

Explanation

Use Publish Code Coverage Results task in a build pipeline to publish code coverage results to Azure Pipelines or TFS, which were produced by a build in Cobertura or JaCoCo format.

Reference:

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

NO.260 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

Explanation

<https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/github?view=azure-devops&tabs=yaml>

<https://developer.github.com/v3/checks/>

NO.261 Your company uses a Git repository in Azure Repos to manage the source code of a web application. The master branch is protected from direct updates. Developers work on new features in the topic branches.

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

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

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

Which merge strategy should you use in the branch policy?

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

Answer: C

Explanation

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

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

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

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

NO.262 You are creating a container for an ASP.NET Core app.

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

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

NOTE: Each correct selection is worth one point.

Answer Area	
Values	
dotnet publish -c Release -o out	FROM [REDACTED] As build-env
dotnet restore	COPY . /app/
microsoft/dotnet:2.2-aspnetcore-runtime	WORKDIR /app
Microsoft/dotnet:2.2-sdk	RUN [REDACTED]
	FROM [REDACTED]
	COPY --from=build-env /app/out /app
	WORKDIR /app
	ENTRYPOINT ["dotnet", "MvcMovie.dll"]

Answer:

Answer Area	
Values	
dotnet publish -c Release -o out	FROM Microsoft/dotnet:2.2-sdk As build-env
dotnet restore	COPY . /app/
microsoft/dotnet:2.2-aspnetcore-runtime	WORKDIR /app
Microsoft/dotnet:2.2-sdk	RUN dotnet restore
	FROM microsoft/dotnet:2.2-aspnetcore-runtime
	COPY --from=build-env /app/out /app
	WORKDIR /app
	ENTRYPOINT ["dotnet", "MvcMovie.dll"]

Explanation

```

FROM Microsoft/dotnet:2.2-sdk As build-env
COPY . /app/
WORKDIR /app
RUN dotnet restore
FROM microsoft/dotnet:2.2-aspnetcore-runtime
COPY --from=build-env /app/out /app
WORKDIR /app
ENTRYPOINT ["dotnet", "MvcMovie.dll"]

```

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>

NO.263 You are creating a NuGet package.

You plan to distribute the package to your development team privately.

You need to share the package and test that the package can be consumed.

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

Actions

Answer Area

Create a new Azure Artifacts feed.

Configure a self-hosted agent.

Publish a package.

Install a package.

Connect to an Azure Artifacts feed.



Answer:

Actions

Create a new Azure Artifacts feed.

Configure a self-hosted agent.

Publish a package.

Install a package.

Connect to an Azure Artifacts feed.

Answer Area

Configure a self-hosted agent.

Create a new Azure Artifacts feed.

Publish a package.

Connect to an Azure Artifacts feed.

**Explanation**

Configure a self-hosted agent.

Create a new Azure Artifacts feed.

Publish a package.

Connect to an Azure Artifacts feed.

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>

NO.264 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.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various navigation items like Home, Dashboard, and DevTest Labs. The 'All services' item is highlighted with a red box and a yellow circle containing the number '1'. In the main content area, there are several sections: 'SECURITY', 'DEVOPS', and 'MIGRATE'. Under 'DEVOPS', the 'DevTest Labs' service is listed with a yellow circle containing the number '2'. At the bottom of the page, there's another 'DevTest Labs' item in the navigation bar, also highlighted with a yellow circle containing the number '3'.

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>

NO.265 During a code review, you discover many quality issues. Many modules contain unused variables and empty catch Modes. You need to recommend a solution to improve the quality o' the code. What should you recommend?

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

Answer: D

Explanation

PMD is a source code analyzer. It finds common programming flaws like unused variables, empty catch blocks, unnecessary object creation, and so forth.

There is an Apache Maven PMD Plugin which allows you to automatically run the PMD code analysis

tool on your project's source code and generate a site report with its results.

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

NO.266 You have an Azure Kubernetes Service (AKS) cluster.

You need to deploy an application to the cluster by using Azure DevOps.

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

Answer Area

Actions

Create a service account in the cluster.

Create a service principal in Azure Active Directory (Azure AD).

Add an Azure Function App for Container task to the deployment pipeline.

Add a Helm package and deploy a task to the deployment pipeline.

Add a Docker Compose task to the deployment pipeline.

Configure RBAC roles in the cluster.

Answer:

Answer Area

Actions

Create a service account in the cluster.

Create a service principal in Azure Active Directory (Azure AD).

Add an Azure Function App for Container task to the deployment pipeline.

Add a Helm package and deploy a task to the deployment pipeline.

Add a Docker Compose task to the deployment pipeline.

Configure RBAC roles in the cluster.

Explanation

Create a service principal in Azure Active Directory (Azure AD).

Add a Helm package and deploy a task to the deployment pipeline.

Add a Docker Compose task to the deployment pipeline.

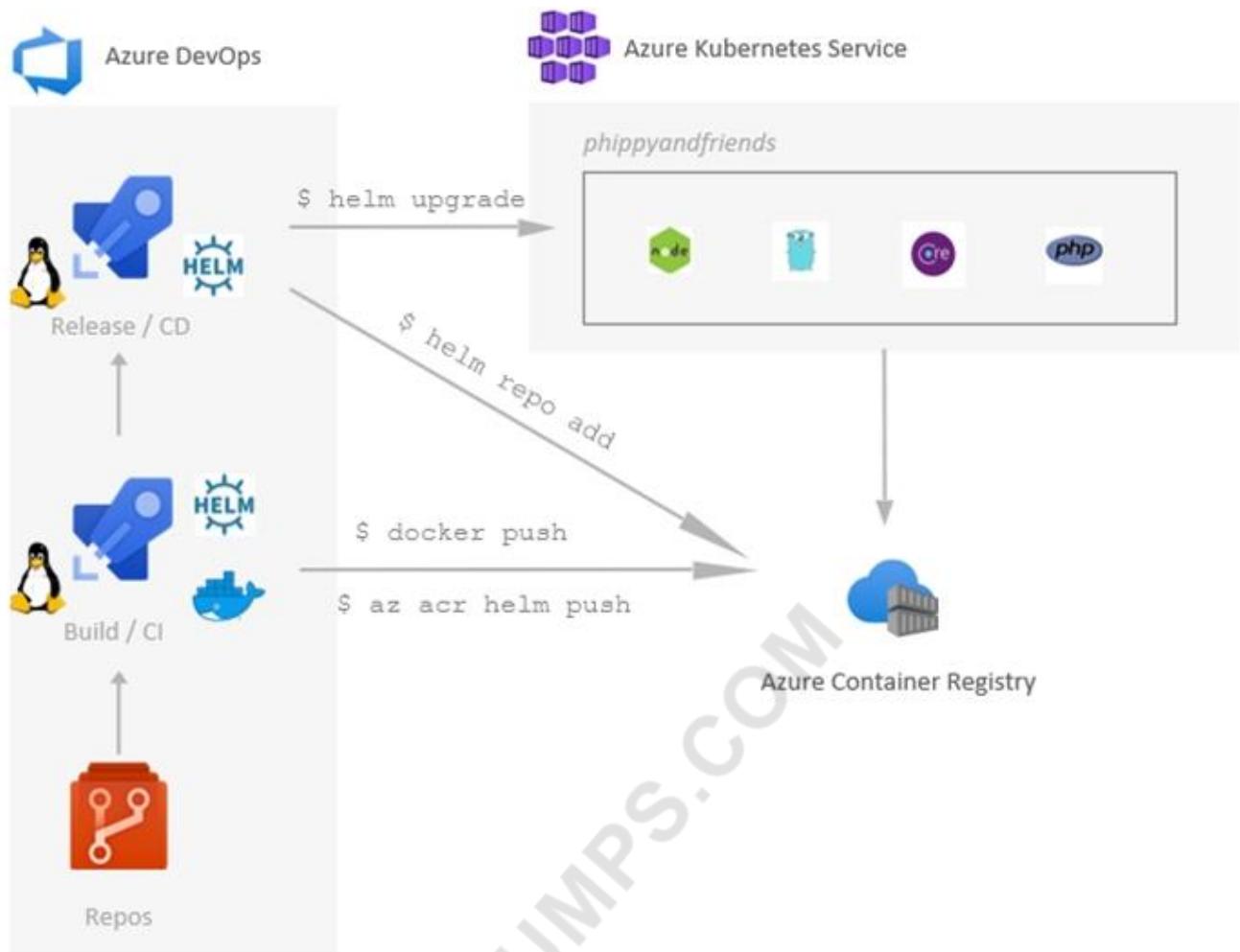
You can set up a CI/CD pipeline to deploy your apps on a Kubernetes cluster with Azure DevOps by leveraging a Linux agent, Docker, and Helm.

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>

NO.267 You have a protect in Azure DevOps.

You need to associate an automated test to a test case.

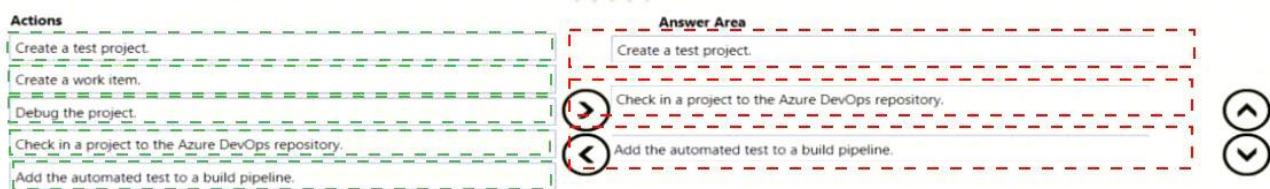
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions
Create a test project.
Create a work item.
Debug the project.
Check in a project to the Azure DevOps repository.
Add the automated test to a build pipeline.

Answer Area



Answer:



Explanation

Answer Area

- 1 Create a test project.
- 2 Check in a project to the Azure DevOps repository.
- 3 Add the automated test to a build pipeline.

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>

NO.268 You are designing YAML-based Azure pipelines for the apps shown in the following table.

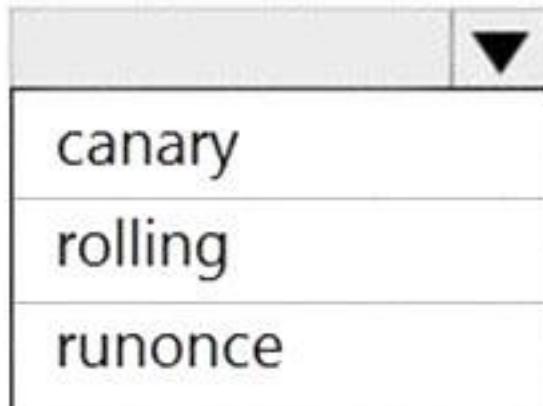
Name	Platform	Release requirements
App1	Azure virtual machine	Replace a fixed set of existing instances of the previous version of App1 with instances of the new version of the app in each iteration.
App2	Azure Kubernetes Service (AKS) cluster	Roll out a limited deployment of the new version of App2 to validate the functionality of the app. Once testing is successful, expand the rollout.

You need to configure the YAML strategy value for each app. The solution must minimize app downtime.

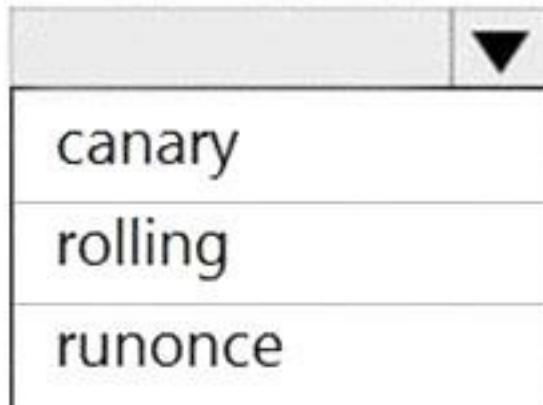
Which value should you configure for each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

App1:

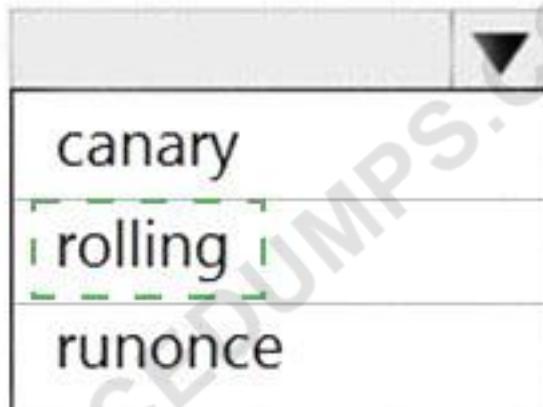


App2:

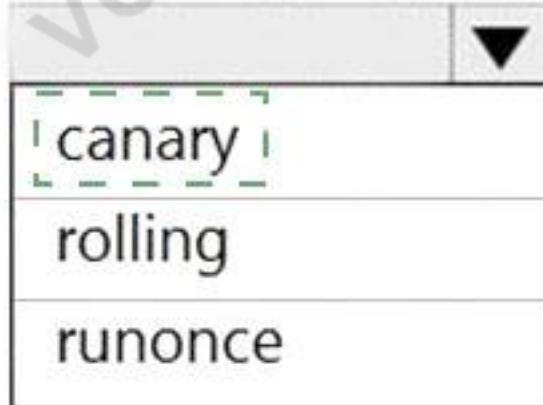


Answer:

App1:

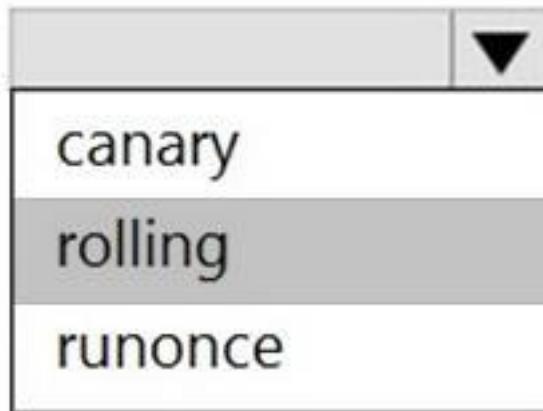


App2:

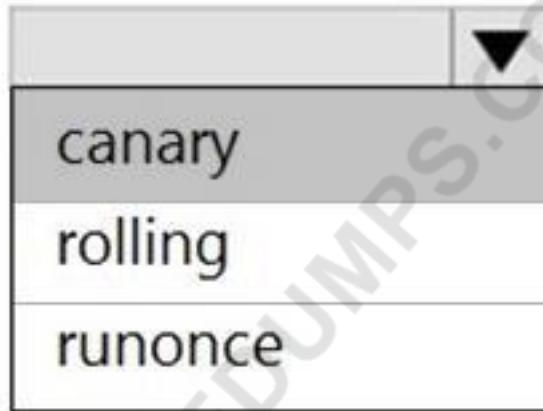


Explanation

App1:



App2:



App1: rolling

A rolling deployment replaces instances of the previous version of an application with instances of the new version of the application on a fixed set of virtual machines (rolling set) in each iteration.

App2: canary

Canary deployment strategy is an advanced deployment strategy that helps mitigate the risk involved in rolling out new versions of applications. By using this strategy, you can roll out the changes to a small subset of servers first. As you gain more confidence in the new version, you can release it to more servers in your infrastructure and route more traffic to it.

Reference:

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

NO.269 unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution After you answer a question in this section, you will NOT be able to return to it. As a result these questions will not appear in the review screen.

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

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

Solution: You create a service hook subscription that uses the build completed event Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation

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

However, the service subscription event should use the code pushed event, is triggered when the code is pushed to a Git repository.

NO.270 You are implementing an Azure DevOps strategy for mobile devices using App Center.

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Private

Public

Shared

Group1:

Group2:

Group3:

Answer:

Answer Area

Private
Public
Shared



Group1: Private
Group2: Public
Group3: Shared

Explanation

Group1: Private
Group2: Public
Group3: Shared

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>

NO.271 You have an Azure DevOps project that contains a build pipeline. The build pipeline uses approximately 50 open source libraries.

You need to ensure that all the open source libraries comply with your company's licensing

standards.

Which service should you use?

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

Answer: C

Explanation

Secure and Manage Open Source Software

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

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

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

Reference:

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

NO.272 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 an Xcode build task, select Use xcpretty from Advanced.
- B. In a Maven build task, select Run PMD.
- C. In a Grunt build task, select Enabled from Control Options.
- D. In a Gulp build task, specify a custom condition expression.

Answer: B

NO.273 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 organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 that is configured for autoscaling.

You have a project in Azure DevOps named Project1. Project1 is used to build a web app named App1 and deploy App1 to VMSS1.

You need to ensure that an email alert is generated whenever VMSS1 scales in or out.

Solution: From Azure Monitor, create an action group.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NO.274 Your company has two virtual machines that run Linux in a third-party public cloud.

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

You need to onboard the Linux virtual machines.

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

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

Answer:

Explanation

Step 1: Create a DSC metaconfiguration

Load up the DSC Configuration into Azure Automation.

Step 2: Copy the metaconfiguration to the virtual machines.

Linking the Node Configuration to the Linux Host

Step 3: Add the virtual machines as DSC nodes in Azure Automation.

go to DSC Nodes, select your node, and then click Assign node configuration. This step assigns the DSC configuration to the Linux machine.

Next up will be to link the node configuration to the host. Go to the host and press the "Assign node..."-button. Next up you can select your node configuration.

Topic 2, Case Study: 2Overview

Existing Environment

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

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
Project 1	Project1 will provide support for incremental builds and third-party SDK components
Project 2	Project2 will use an automatic build policy. A small team of developers named Team2 will work independently on changes to the project. The Team2 members will not have permissions to Project2.
Project 3	Project3 will be integrated with SonarQube
Project 4	Project4 will provide support for a build pipeline that creates a Docker image and pushes the image to the Azure Container Registry. Project4 will use an existing Dockerfile.
Project 5	Project5 will contain a Git repository in Azure Reports and a continuous integration trigger that will initiate a build in response to any change except for changes within /folder1 of the repository.
Project 6	Project6 will provide support for build and deployment pipelines. Deployment will be allowed only if the number of current work items representing active software bugs is 0.
Project 7	Project7 will contain a target deployment group named Group7 that maps to Pool7. Project7 will use Azure Automation State Configuration to maintain the desired state of the computers in Group7.

Technical Requirements

Contoso identifies the following technical requirements:

- * Implement build agents for 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 Team2 on a copy of Project2 will be subject to the same restrictions as the ones defined in the build policy of Project2.
 - * Whenever possible, implement automation and minimize administrative effort.
 - * Implement Project3, Project5, Project6, and Project7 based on the planned changes.
 - * Implement Project4 and configure the project to push Docker images to Azure Container Registry.

NO.275 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

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.

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/>

NO.276 You need to implement the code flow strategy for Project2 in Azure DevOps.

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

Actions

- Create a repository
- Add a build policy for the fork.
- Create a branch.
- Add a build policy for the master branch.
- Add an application access policy.
- Create a fork.

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

- Create a repository
- Add a build policy for the fork.
- Create a branch.
- Add a build policy for the master branch.
- Add an application access policy.
- Create a fork.

Answer Area

- Create a repository
- Add a build policy for the master branch.
- Create a branch.

Explanation**Answer Area**

Create a repository

Add a build policy for the master branch.

Create a branch.

NO.277 You need to configure Azure Automation for the computers in Pool7.

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

Actions	Answer Area
Run the New-AzureRmResourceGroupDeployment Azure PowerShell cmdlet.	1
Create an Azure Resource Manager template file that has an extension of .json.	2
Run the Import-AzureRmAutomationDscConfiguration Azure PowerShell cmdlet.	3
Run the Start-AzureRmAutomationDscCompilationJob Azure PowerShell cmdlet.	
Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1.	

↓

Answer:

Actions	Answer Area
Run the New-AzureRmResourceGroupDeployment Azure PowerShell cmdlet.	1 Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1.
Create an Azure Resource Manager template file that has an extension of .json.	2 Run the Import-AzureRmAutomationDscConfiguration Azure PowerShell cmdlet.
Run the Import-AzureRmAutomationDscConfiguration Azure PowerShell cmdlet.	3 Run the Start-AzureRmAutomationDscCompilationJob Azure PowerShell cmdlet.
Run the Start-AzureRmAutomationDscCompilationJob Azure PowerShell cmdlet.	
Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1.	

↓

Explanation

Actions

Run the `New-AzureRmResourceGroupDeployment` Azure PowerShell cmdlet.

Create an Azure Resource Manager template file that has an extension of .json.

Answer Area

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

2 Run the `Import-AzureRmAutomationDscConfiguration` Azure PowerShell cmdlet.

3 Run the `Start-AzureRmAutomationDscCompilationJob` Azure PowerShell cmdlet.



NO.278 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.

Set a

/folder1.	▼
branch filter to exclude	
branch filter to include	
path filter to exclude	
path filter to include	

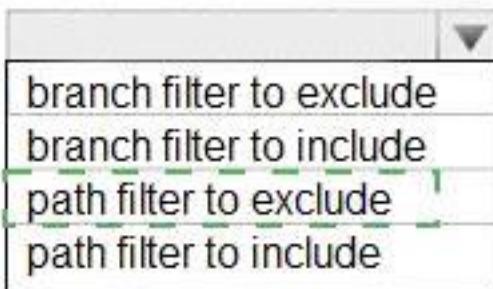
Set a

/.	▼
branch filter to exclude	
branch filter to include	
path filter to exclude	
path filter to include	

@

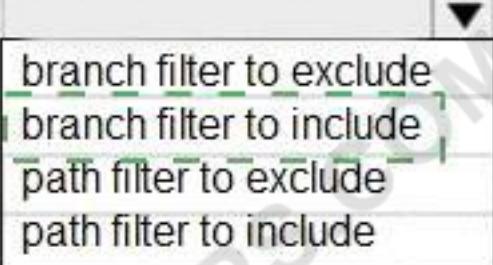
Answer:

Set a



/folder1.

Set a

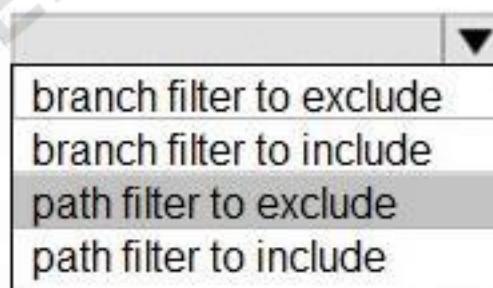


/

@

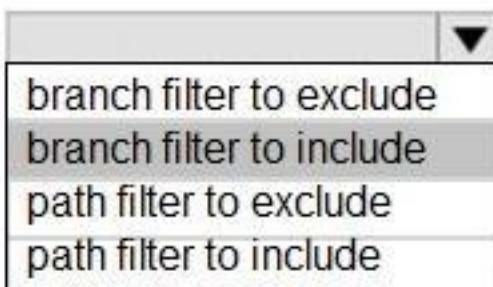
Explanation

Set a



/folder1.

Set a



/

@

Scenario:

Project5 will contain a Git repository in Azure Reports and a continuous integration trigger that will initiate a build in response to any change except for changes within /folder1 of the repository.

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

NO.279 You add the virtual machines as managed nodes in Azure Automation State Configuration.

You need to configure the computer in Group7.

What should you do?

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

Answer: A

Explanation

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

Scenario: The Azure DevOps organization includes:

The Docker extension

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

NO.280 In Azure DevOps, you create Project3.

You need to meet the requirements of the project.

What should you do first?

- A.** From Azure DevOps, create a service endpoint.
- B.** From SonarQube, obtain an authentication token.
- C.** From Azure DevOps, modify the build definition.
- D.** From SonarQube, create a project.

Answer: A

Explanation

The first thing to do is to declare your SonarQube server as a service endpoint in your VSTS/DevOps project settings.

References:

<https://docs.sonarqube.org/display/SCAN/Analyzing+with+SonarQube+Extension+for+vsts-TFS>

NO.281 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.

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

Answer:

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

Explanation

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

Run the `Import-AzureRmAutomationDscConfiguration` Azure PowerShell cmdlet.

Run the `Start-AzureRmAutomationDscCompilationJob` Azure PowerShell cmdlet.

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>

NO.282 You need to implement Project4.

What should you do first?

- A. Add the FROM instruction in the Dockerfile file.
- B. Add a Copy and Publish Build Artifacts task to the build pipeline.
- C. Add a Docker task to the build pipeline.
- D. Add the MAINTAINER instruction in the Dockerfile file.

Answer: C

Explanation

Scenario: Implement Project4 and configure the project to push Docker images to Azure Container Registry.

Project 4

Project4 will provide support for a build pipeline that creates a Docker image and pushes the image to the Azure Container Registry. Project4 will use an existing Dockerfile.

You use Azure Container Registry Tasks commands to quickly build, push, and run a Docker container image natively within Azure, showing how to offload your "inner-loop" development cycle to the cloud. ACR Tasks is a suite of features within Azure Container Registry to help you manage and modify container images across the container lifecycle.

References:

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

NO.283 You need to implement Project6.

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

Actions

- Open the release pipeline editor.
- Open the **Triggers** tab.
- Disable the continuous integration trigger.
- Enable Gates.
- Add a manual intervention task.
- Add Query Work Items.

Answer Area

- 1
- 2
- 3

**Answer:****Actions**

- Open the release pipeline editor.
- Open the **Triggers** tab.
- Disable the continuous integration trigger.
- Enable Gates.
- Add a manual intervention task.
- Add Query Work Items.

Answer Area

- 1 Open the release pipeline editor.
- 2 Enable Gates.
- 3 Add Query Work Items.

**Explanation**

Open the release pipeline editor.

Enable Gates.

Add Query Work Items.

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.

VCEDUMPS.COM

Deployment gates ⓘ

+ Add ⚙

Query Work Items

Enabled

Query Work Items ⓘ

Task version 0.* ▾

Display name *

Query Work Items

Query * ⓘ

Active Bugs ▾

Upper threshold * ⓘ

0

Advanced ▾

Lower threshold * ⓘ

0

Output Variables ▾

Reference name ⓘ

Variables list

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

Evaluation options ▾

Note: A case for release gate is:

Incident and issues management. Ensure the required status for work items, incidents, and issues.

For example, ensure deployment occurs only if no priority zero bugs exist, and validation that there are no active incidents takes place after deployment.

References:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deploy-using-approvals?view=azure-devops#co>

NO.284 You need to implement the code flow strategy for Project2 in Azure DevOps.

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

Actions	Answer Area
Create a fork	
Create a branch	
Add a build validation policy.	(Left Arrow)
Add a build policy	(Right Arrow)
Create a repository	
Add an application access policy.	

Answer:

Actions	Answer Area
Create a fork	
Create a branch	
Add a build validation policy.	(Left Arrow)
Add a build policy	(Right Arrow)
Create a repository	Create a repository
	Create a branch
	Add a build validation policy.

Explanation

Answer Area

Create a repository

Create a branch

Add a build validation policy.

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>