



CertyIQ

Premium exam material

Get certification quickly with the CertyIQ Premium exam material.
Everything you need to prepare, learn & pass your certification exam easily. Lifetime free updates
First attempt guaranteed success.

<https://www.CertyIQ.com>



About CertyIQ

We here at CertyIQ eventually got enough of the industry's greedy exam paid for. Our team of IT professionals comes with years of experience in the IT industry Prior to training CertiIQ we worked in test areas where we observed the horrors of the paywall exam preparation system.

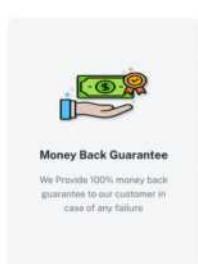
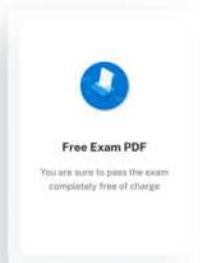
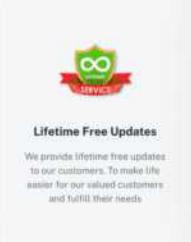
The misuse of the preparation system has left our team disillusioned. And for that reason, we decided it was time to make a difference. We had to make In this way, CertyIQ was created to provide quality materials without stealing from everyday people who are trying to make a living.

Doubt Support

We have developed a very scalable solution using which we are able to solve 400+ doubts every single day with an average rating of 4.8 out of 5.

<https://www.certyiq.com>

Mail us on - certyiqofficial@gmail.com



John

October 19, 2022



Thanks you so much for your help. I scored 972 in my exam today. More than 90% were from your PDFs!

October 22, 2022



Passed my exam today with 891 marks. Out of 52 questions, 51 were from certyiq PDFs including Contoso case study.

Thank You certyiq team!

Dana

September 04, 2022



Thanks a lot for this updated AZ-900 Q&A. I just passed my exam and got 974, I followed both of your Az-900 videos and the 6 PDF, the PDFs are very much valid, all answers are correct. Could you please create a similar video/PDF for DP900, your content/PDF's is really awesome. The team did a really good job. Thank You 😊.

Henry Rome

2 months ago



These questions are real and 100 % valid. Thank you so much for your efforts, also your 4 PDFs are awesome, I passed the DP900 exam on 1 Sept. With 968 marks. Thanks a lot, buddy!

Esmaria

2 months ago



Simple easy to understand explanations. To anyone out there wanting to write AZ900, I highly recommend 6 PDF's. Thank you so much, appreciate all your hard work in having such great content. Passed my exam Today - 3 September with 942 score.

Ahamed Shibly

2 months ago



Customer support is realy fast and helpful, I just finished my exam and this video along with the 6 PDF helped me pass! Definitely recommend getting the PDFs. Thank you!



(AZ-400)

Microsoft Azure DevOps Solutions

Total: **502 Questions**

Link: <https://certiq.com/papers?provider=microsoft&exam=az-400>

Question: 1

CertyIQ

You are configuring project metrics for dashboards in Azure DevOps.

You need to configure a chart widget that measures the elapsed time to complete work items once they become active.

Which of the following is the widget you should use?

- A. Cumulative Flow Diagram
- B. Burnup
- C. Cycle time**
- D. Burndown

Answer: C

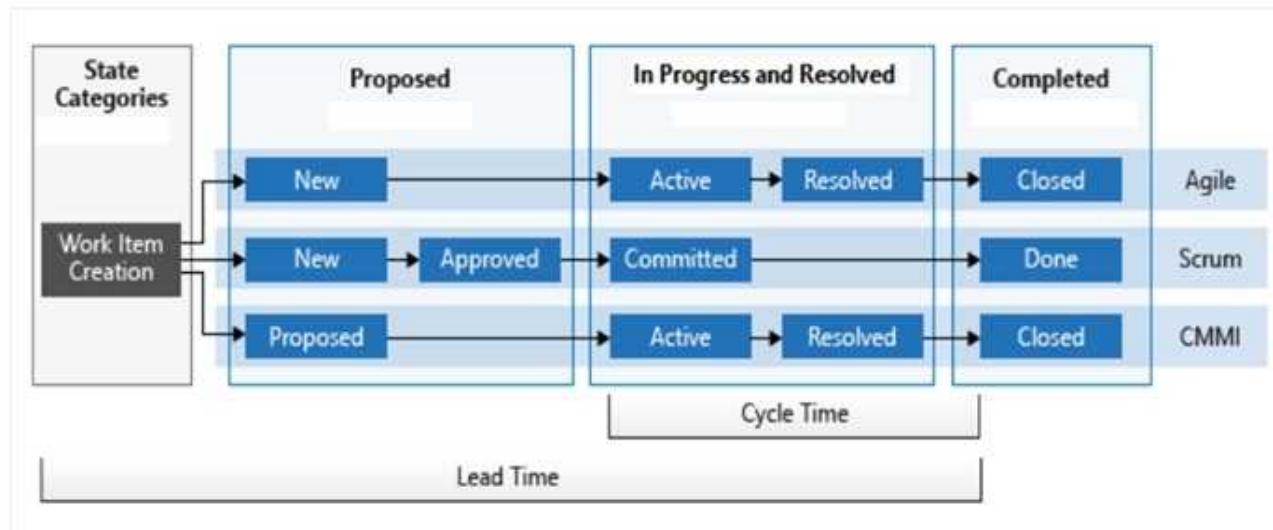
Explanation:

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

Reference:

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

The following diagram illustrates how lead time differs from cycle time. Lead time is calculated from work item creation to entering a completed state. Cycle time is calculated from first entering an In Progress or Resolved state category to entering a Completed state category. To understand how workflow states map to state categories, see [How workflow states and state categories are used in Backlogs and Boards](#).



Question: 2

CertyIQ

You need to consider the underlined segment to establish whether it is accurate.

The Burnup widget measures the elapsed time from creation of work items to their completion.

Select 'No adjustment required' if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

- A. No adjustment required.
- B. Lead time**

- C. Test results trend
- D. Burndown

Answer: B

Explanation:

Reference:

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

Question: 3

CertyIQ

You are making use of Azure DevOps manage build pipelines, and also deploy pipelines. The development team is quite large, and is regularly added to. You have been informed that the management of users and licenses must be automated when it can be. Which of the following is a task that can't be automated?

- A. Group membership changes
- B. License assignment
- C. Assigning entitlements
- D. License procurement

Answer: D

Explanation:

1. Answer is D .Group membership can be dynamic hence are automated

Question: 4

CertyIQ

You have been tasked with strengthening the security of your team's development process. You need to suggest a security tool type for the Continuous Integration (CI) phase of the development process. Which of the following is the option you would suggest?

- A. Penetration testing
- B. Static code analysis
- C. Threat modeling
- D. Dynamic code analysis

Answer: B

Explanation:

Validation in the CI/CD begins before the developer commits his or her code. Static code analysis tools in the IDE provide the first line of defense to help ensure that security vulnerabilities are not introduced into the CI/CD process.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/articles/security-validation-cicd-pipeline?view=vsts>
" target="_blank" style="word-break: break-all;">>

Note

Azure Pipelines is one among a collection of Azure DevOps Services, all built on the same secure infrastructure in Azure. To understand the main concepts around security for all of Azure DevOps Services, see [Azure DevOps Data Protection Overview](#) and [Azure DevOps Security and Identity](#).

Traditionally, organizations implemented security through draconian lock-downs. Code, pipelines, and production environments had severe restrictions on access and use. In small organizations with a few users and projects, this stance was relatively easy to manage. However, that's not the case in larger organizations. Where many users have contributor access to code, one must "assume breach". Assuming breach means behaving as if an adversary has contributor access to some (if not all) of the repositories.

Question: 5

CertyIQ

Your company is currently making use of Team Foundation Server 2013 (TFS 2013), but intend to migrate to Azure DevOps.

You have been tasked with supplying a migration approach that allows for the preservation of Team Foundation Version Control changesets dates, as well as the changes dates of work items revisions. The approach should also allow for the migration of all TFS artifacts, while keeping migration effort to a minimum.

You have suggested upgrading TFS to the most recent RTW release.

Which of the following should also be suggested?

- A. Installing the TFS kava SDK
- B. **Using the TFS Database Import Service to perform the upgrade.**
- C. Upgrading PowerShell Core to the latest version.
- D. Using the TFS Integration Platform to perform the upgrade.

Answer: B

Explanation:

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.

Question: 6

CertyIQ

DRAG DROP -

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

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

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

Select and Place:

Options

Answer

A self-hosted agent

A Microsoft-hosted agent

An External Git service connection

Service hooks

Answer:

Options

Answer

A self-hosted agent

A Microsoft-hosted agent

An External Git service connection

Service hooks

A self-hosted agent

An External Git service connection

Explanation:

Reference:

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

" target="_blank" style="word-break: break-all;">>

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

Question: 7

You are currently developing a project for a client that will be managing work items via Azure DevOps. You want to make sure that the work item process you use for the client allows for requirements, change requests, risks, and reviews to be tracked.

Which of the following is the option you would choose?

- A. Basic
- B. Agile
- C. Scrum
- D. CMMI

Answer: D**Explanation:**

Choose CMMI when your team follows more formal project methods that require a framework for process improvement and an auditable record of decisions. With this process, you can track requirements, change requests, risks, and reviews.

Incorrect Answers:

- A. Choose Basic when your team wants the simplest model that uses Issues, Tasks, and Epics to track work.
- B. 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.
- C. 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.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/boards/work-items/guidance/choose-process?view=azure-devops>

Question: 8

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

You run the Register-AzureRmAutomationDscNode command in your company's environment.

You need to make sure that your company's test servers remain correctly configured, regardless of configuration drift.

Solution: You set the -ConfigurationMode parameter to ApplyOnly.

Does the solution meet the goal?

- A. Yes
- B. No

Answer: B**Explanation:**

Reference:

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

" target="_blank" style="word-break: break-all;">>

Register-AzureRmAutomationDscNode

Module: [AzureRM.Automation](#)

Registers an Azure virtual machine as a DSC node for an Automation account.

ⓘ Important

Because Az PowerShell modules now have all the capabilities of AzureRM PowerShell modules and more, we'll retire AzureRM PowerShell modules on 29 February 2024.

To avoid service interruptions, [update your scripts](#) that use AzureRM PowerShell modules to use Az PowerShell modules by 29 February 2024. To automatically update your scripts, follow the [quickstart guide](#).

Question: 9

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

You run the Register-AzureRmAutomationDscNode command in your company's environment.

You need to make sure that your company's test servers remain correctly configured, regardless of configuration drift.

Solution: You set the -ConfigurationMode parameter to ApplyAndMonitor.

Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Reference:

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

Question: 10

CertyIQ

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

You run the Register-AzureRmAutomationDscNode command in your company's environment.

You need to make sure that your company's test servers remain correctly configured, regardless of configuration drift.

Solution: You set the -ConfigurationMode parameter to ApplyAndAutocorrect.

Does the solution meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Reference:

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

CertyIQ

Question: 11

You need to consider the underlined segment to establish whether it is accurate.

To compile an Internet Information Services (IIS) web application that runs docker, you should use a Default build agent pool.

Select 'No adjustment required' if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

- A. No adjustment required.
- B. Hosted Windows Container**
- C. Hosted
- D. Hosted macOS

Answer: B

Explanation:

Hosted windows container is a correct answer

CertyIQ

Question: 12

Your company has an Azure DevOps environment that can only be accessed by Azure Active Directory users.

You are instructed to make sure that the Azure DevOps environment can only be accessed from devices connected to the company's on-premises network.

Which of the following actions should you take?

- A. Assign the devices to a security group.
- B. Create a GPO.
- C. Configure Security in Project Settings from Azure DevOps.
- D. Configure conditional access in Azure Active Directory.**

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.

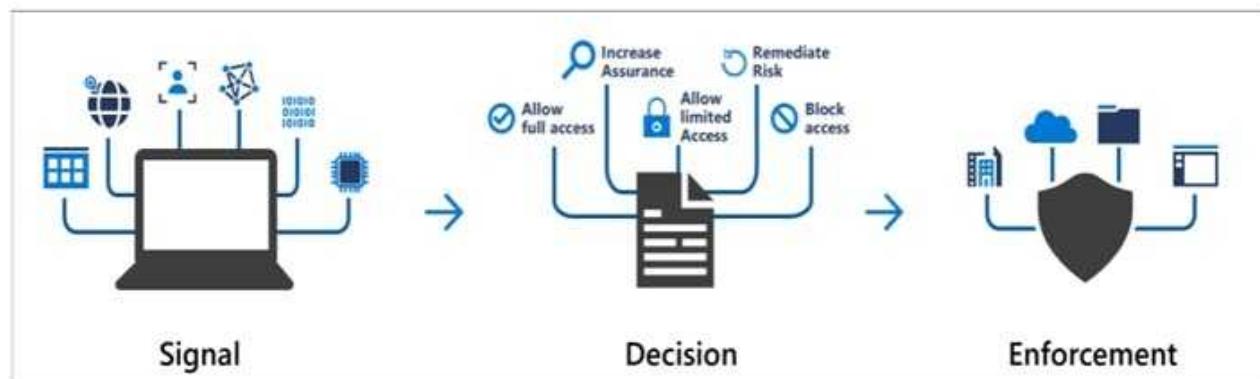
Conditional Access policies are enforced after the first-factor authentication has been completed.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

" target="_blank" style="word-break: break-all;">>

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.



Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it.

Administrators are faced with two primary goals:

Question: 13

CertyIQ

You are making use of Azure DevOps to configure Azure Pipelines for project, named PROJ-01.

You are preparing to use a version control system that allows for source code to be stored on a managed Windows server located on the company network.

Which of the following is the version control system you should use?

- A. Github Enterprise
- B. Bitbucket cloud
- C. Github Professional
- D. Git in Azure Repos

Answer: A

Explanation:

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).

Reference:

<https://www.azuredevopslabs.com/labs/azuredevops/yaml/>

[https://enterprise.github.com/faq" target="_blank" style="word-break: break-all;">](https://enterprise.github.com/faq)

Pipelines as Code with YAML



<https://enterprise.github.com/faq>

Question: 14

CertyIQ

You need to consider the underlined segment to establish whether it is accurate.
When moving to Azure DevOps, JIRA must be replaced with the build pipelines Azure DevOps service.
Select 'No adjustment required' if the underlined segment is accurate. If the underlined segment is inaccurate,
select the accurate option.

- A. No adjustment required.
- B. repos
- C. release pipelines
- D. boards

Answer: D

Explanation:

Jira is task management tool can be replaced with Azure boards which fulfils similar goals

Question: 15

CertyIQ

You scan a Node.js application using WhiteSource Bolt.
The scan finds numerous libraries with invalid licenses, but are only used during development.
You have to make sure that only production dependencies are scanned by WhiteSource Bolt.
Which of the following is a command you should run?

- A. npm edit
- B. npm publish
- C. **npm install**
- D. npm update

Answer: C

Explanation:

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>

Question: 16

CertyIQ

You are currently defining a release strategy for an app, named APP-01.

The strategy should allow you to keep the time it takes to deploy new releases of the app to a minimum. The strategy should also allow you to roll back in the shortest time required.

Which of the following is the release strategy you should use?

- A. Red/Black deployment
- B. Rolling deployment
- C. Big Bang deployment
- D. Canary deployment

Answer: A

Explanation:

Blue/green and Red/Black are same. Must be 2 ['coloured' paths] to swap immediately between them. Read the line "The strategy should also allow you to roll back in the shortest time required So answer is A.

Question: 17

CertyIQ

Your company hosts a web application in Azure, and makes use of Azure Pipelines for managing the build and release of the application.

When stakeholders report that system performance has been adversely affected by the most recent releases, you configure alerts in Azure Monitor.

You are informed that new releases must satisfy specified performance baseline conditions in the staging environment before they can be deployed to production.

You need to make sure that releases not satisfying the performance baseline are prevented from being deployed. Which of the following actions should you take?

- A. You should make use of a branch control check.
- B. You should make use of an alert trigger.
- C. You should make use of a gate.
- D. You should make use of an approval check.

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.

Reference:

<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>

Question: 18

CertyIQ

You need to consider the underlined segment to establish whether it is accurate.

To deploy an application to a number of Azure virtual machines, you should create a universal group.

Select 'No adjustment required' if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. security

C. deployment

D. resource

Answer: C

Explanation:

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.

Reference:

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

" target="_blank" style="word-break: break-all;">>

[Azure Pipelines](#) | [Azure DevOps Server 2020](#) | [Azure DevOps Server 2019](#) | [TFS 2018](#)

A deployment group is a logical set of deployment target machines that have agents installed on each one. Deployment groups represent the physical environments; for example, "Dev", "Test", or "Production" environment. In effect, a deployment group is just another grouping of agents, much like an agent pool.

Deployment groups are only available with Classic release pipelines and are different from deployment jobs. A deployment job is a collection of deployment-related steps defined in a YAML file to accomplish a specific task.

With deployment groups you can:

- Specify the security context and runtime targets for the agents. As you create a deployment group, you add users and give them appropriate permissions to administer, manage, view, and use the group.

Question: 19

DRAG DROP -

You are preparing to deploy an Azure resource group via Terraform.

To achieve your goal, you have to install the necessary frameworks.

Which of the following are the frameworks you should use? Answer by dragging the correct options from the list to the answer area.

Select and Place:

Options

Yeoman

Vault

Terratest

Tiller

Answer

Answer:

Options

Yeoman

Vault

Terratest

Tiller

Answer

Yeoman

Terratest

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>

Question: 20

You intend to make use of Azure Artifacts to share packages that you wrote, tested, validated, and deployed. You want to use a solitary feed to release several builds of each package. You have to make sure that the release of packages that are in development is restricted.

Which of the following actions should you take?

- A. You should make use of static code analysis.
- B. You should make use of views.**
- C. You should make use of dynamic code analysis.
- D. You should make use of upstream sources.

Answer: B

Explanation:

Feed views enable developers to share a subset of package-versions with their consumers. A common use of feed views is to share package versions that have been tested and validated but hold back on packages that are still under development and/or didn't meet a certain quality bar.

Feed views and upstream sources are designed to work together to provide an enterprise-level solution to share and consume packages. In order for other Azure Artifacts feeds to use your feed as an upstream source, you must set your feed's visibility to members of your organization, or members of your Azure Active Directory, depending on your scenario. If you choose the latter, all people in your organization will be able to access your feed, and all feeds in your organization and other organizations associated with the same Azure Active Directory tenant will be able to upstream to your feed.

Question: 21

CertyIQ

You need to consider the underlined segment to establish whether it is accurate.

To find when common open source libraries are added to the code base, you should add Jenkins to the build pipeline.

Select 'No adjustment required' if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

- A. No adjustment required.
- B. SourceGear Vault
- C. WhiteSource**
- D. OWASP ZAP

Answer: C

Explanation:

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

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

Azure DevOps integration with WhiteSource Bolt will enable you to:

1. Detect and remedy vulnerable open source components.
2. Generate comprehensive open source inventory reports per project or build.
3. Enforce open source license compliance, including dependencies' licenses.
4. Identify outdated open source libraries with recommendations to update.

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

Reference:

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

Question: 22

CertyIQ

Your company has an Azure DevOps project, which includes a build pipeline that makes use of roughly fifty open source libraries.

You have been tasked with making sure that you are able to scan project for common security weaknesses in the open source libraries.

Which of the following actions should you take?

- A. You should create a build task and use the WhiteSource Bolt service.
- B. You should create a deployment task and use the WhiteSource Bolt service.
- C. You should create a build task and use the Chef service.
- D. You should create a deployment task and use the Chef service.

Answer: A**Explanation:**

whitesource is the tool and it should be used on CI phase.

Reference:

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

Question: 23

CertyIQ

You need to consider the underlined segment to establish whether it is accurate.

Black Duck can be used to make sure that all the open source libraries conform to your company's licensing criteria.

Select 'No adjustment required' if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

- A. No adjustment required.
- B. Maven
- C. Bamboo
- D. CMAKE

Answer: A**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.

Reference:

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

Question: 24

CertyIQ

You have created an Azure DevOps project for a new application that will be deployed to a number of Windows Server 2016 Azure virtual machines.

You are preparing a deployment solution that allows for the virtual machines to maintain a uniform configuration,

and also keep administrative effort with regards to configuring the virtual machines to a minimum. Which of the following should be part of your solution? (Choose two.)

- A. Azure Resource Manager templates
- B. The PowerShell Desired State Configuration (DSC) extension for Windows
- C. Azure pipeline deployment groups
- D. The Custom Script Extension for Windows
- E. Azure pipeline stage templates

Answer: AB

Explanation:

Considering the requirements

- maintain a uniform configuration for virtual machines
- minimize administrative effort

The correct answer is A & B.

To maintain the configuration status of a VM you must use DSC.

To minimize the effort of creating the VM you can use an ARM template so that you can reuse it for each VM. Deployment groups requires more effort.

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-template>

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

Question: 25

CertyIQ

Your company has an application that contains a number of Azure App Service web apps and Azure functions. You would like to view recommendations with regards to the security of the web apps and functions. You plan to navigate to Compute and Apps to achieve your goal.

Which of the following should you access to make use of Compute and Apps?

- A. Azure Log Analytics
- B. Azure Event Hubs
- C. Azure Advisor
- D. 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.

Reference:

Question: 26

You need to consider the underlined segment to establish whether it is accurate.
Your company has a multi-tier application that has its front end hosted in Azure App Service.
To pinpoint the average load times of the application pages, you should make use of Azure Event Hubs.
Select 'No adjustment required' if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

- A. No adjustment required.
- B. Azure Application Insights**
- C. Azure Log Analytics
- D. Azure Advisor

Answer: B

Explanation:

Application Insights will tell you about any performance issues and exceptions, and help you find and diagnose the root causes.
Application Insights can monitor both Java and ASP.NET web applications and services, WCF services. They can be hosted on-premises, on virtual machines, or as Microsoft Azure websites.
On the client side, Application Insights can take telemetry from web pages and a wide variety of devices including iOS, Android, and Windows Store apps.

Reference:

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

Question: 27

Your company makes use of Azure SQL Database Intelligent Insights and Azure Application Insights for monitoring purposes.
You have been tasked with analyzing the monitoring using ad-hoc queries. You need to utilize the correct query language.
Solution: You use the Contextual Query Language (CQL).
Does the solution meet the goal?

- A. Yes
- B. No**

Answer: B

Explanation:

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

Question: 28

Your company makes use of Azure SQL Database Intelligent Insights and Azure Application Insights for monitoring purposes.
You have been tasked with analyzing the monitoring using ad-hoc queries. You need to utilize the correct query language.

Solution: You use the Transact-SQL.

Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Reference:

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

Question: 29

CertyIQ

Your company makes use of Azure SQL Database Intelligent Insights and Azure Application Insights for monitoring purposes.

You have been tasked with analyzing the monitoring using ad-hoc queries. You need to utilize the correct query language.

Solution: You use Azure Log Analytics.

Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:

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

Reference:

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

Question: 30

CertyIQ

DRAG DROP -

You have recently created a web application for your company.

You have been tasked with making sure that a summary of the exceptions that transpire in the application is automatically sent to Microsoft Teams on a daily basis.

Which of the following Azure services should you use? Answer by dragging the correct options from the list to the answer area.

Select and Place:

Options

Answer

Azure DevOps
Project

Azure Logic Apps

Azure Pipelines

Azure Application
Insights

Answer:

Options

Azure DevOps Project

Azure Logic Apps

Azure Pipelines

Azure Application Insights

Answer

Azure Logic Apps

Azure Application Insights

Explanation:

Exceptions in your live web app are reported by Application Insights.

Note: Periodical reports help keep a team informed on how their business critical services are doing.

Developers, DevOps/SRE teams, and their managers can be productive with automated reports reliably delivering insights without requiring everyone to sign in the portal. Such reports can also help identify gradual increases in latencies, load or failure rates that may not trigger any alert rules.

You can programmatically query Application Insights data to generate custom reports on a schedule. The following options can help you get started quickly:

Automate reports with Microsoft Flow

-
- ⇒ Automate reports with Logic Apps

Reference:

<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>

Question: 31

CertyIQ

You are in the process of building a mobile app aimed at Android and iOS devices.

All work items and release cycles are managed via Azure DevOps.

You want to make sure that crash reports for issue analysis is collected, and that beta releases are distributed to your testers. Also, you want to ensure that user feedback on the functionality of new apps is received.

Which of the following must be part of your solution?

- A. The Microsoft Test & Feedback extension.
- B. OWASP ZAP

C. TFS Integration Platform

D. Code Style

Answer: A

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.

Reference:

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

Question: 32

CertyIQ

DRAG DROP -

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.

Select and Place:

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:

Velocity

Answer:

Chart Widgets

Answer Area

Burndown

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

Lead Time

Cycle Time

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

Cycle Time

Lead Time

The remaining work:

Burndown

Explanation:

Box 1: Lead time -

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

Box 2: Cycle time -

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

Box 3: Burndown -

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

Incorrect Answers:

Velocity provides a useful metric for these activities:

Support sprint planning -

Forecast future sprints and the backlog items that can be completed

A guide for determining how well the team estimates and meets their planned commitments

Reference:

<https://docs.microsoft.com/en-us/azure/devops/report/dashboards/velocity-guidance?view=vsts> <https://docs.microsoft.com/en-us/azure/devops/report/dashboards/cycle-time-and-lead-time?view=vsts> <https://docs.microsoft.com/en-us/azure/devops/report/dashboards/configure-burndown-burnup-widgets?view=vsts>

Question: 33

CertyIQ

HOTSPOT -

You plan to create alerts that will be triggered based on the page load performance of a home page.

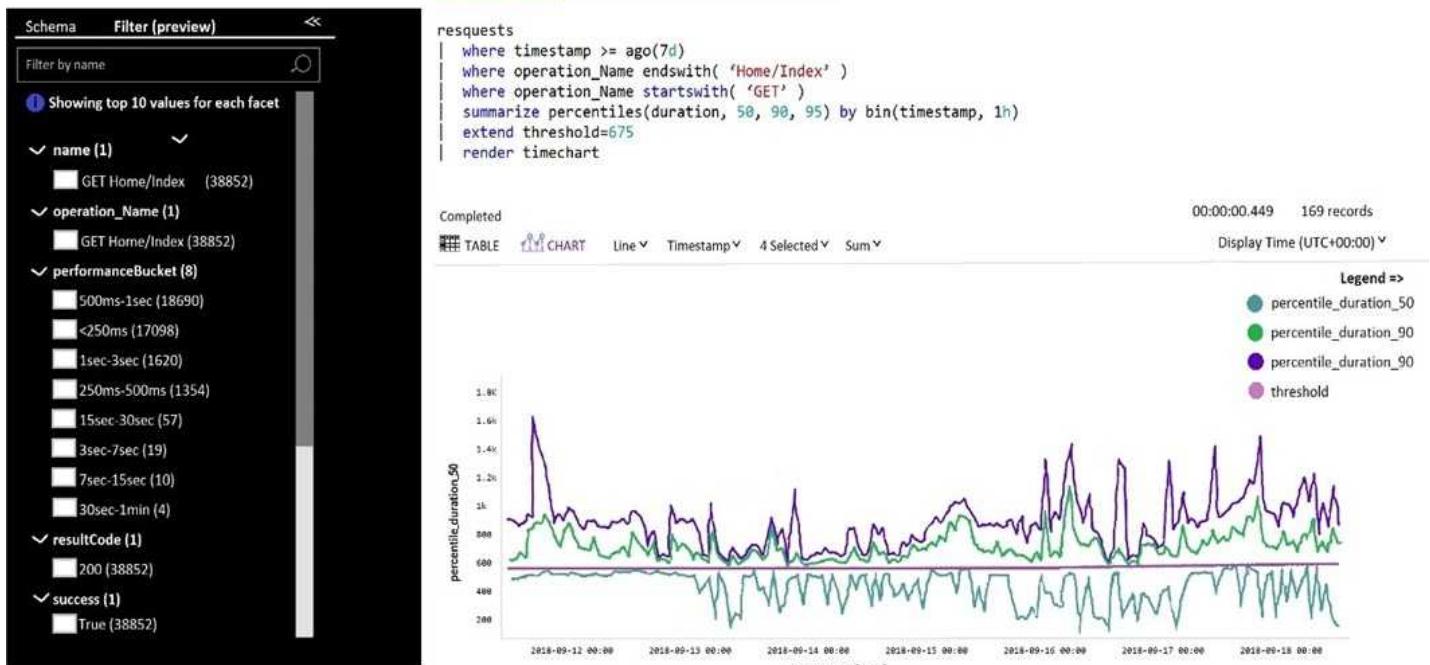
You have the Application Insights log query shown in the following exhibit.

Home Pa... New Query 1* New Query... * X +

Demo

Run

Time range: Set in query



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.

Hot Area:

Answer Area

To create an alert based on the page load experience of most users, the alerting level must be based on [answer choice].

| |
|------------------------|
| percentile.duration.50 |
| percentile.duration.90 |
| percentile.duration.95 |
| threshold |

To only create an alert when authentication error occurs on the server, the query must be filtered on [answer choice].

| |
|------------|
| item Type |
| resultCode |
| source |
| success |

Answer:

Answer Area

To create an alert based on the page load experience of most users, the alerting level must be based on [answer choice].

| |
|------------------------|
| percentile_duration_50 |
| percentile_duration_90 |
| percentile_duration_95 |
| threshold |

To only create an alert when authentication error occurs on the server, the query must be filtered on [answer choice].

| |
|------------|
| item Type |
| resultCode |
| source |
| success |

Explanation:

Box 1: percentile_duration_95 -

Box 2: result code

but the second one is not considering all scenarios.

In App Insight you can check the Request result Code property which will show '403' in case of authentication errors. The answer for the second question should be 'result Code' instead of 'success', as this will ensure that the error is strictly related to authentication.

Question: 34

CertyIQ

You manage an Azure web app that supports an e-commerce website.

You need to increase the logging level when the web app exceeds normal usage patterns. The solution must minimize administrative overhead.

Which two resources should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. an Azure Automation runbook
- B. an Azure Monitor alert that has a dynamic threshold
- C. an Azure Monitor alert that has a static threshold
- D. the Azure Monitor autoscale settings
- E. an Azure Monitor alert that uses an action group that has an email action

Answer: AB

Explanation:

B: Metric Alert with Dynamic Thresholds detection leverages advanced machine learning (ML) to learn metrics' historical behavior, identify patterns and anomalies that indicate possible service issues. It provides support of both a simple UI and operations at scale by allowing users to configure alert rules through the Azure Resource Manager API, in a fully automated manner.

A: You can use Azure Monitor to monitor base-level metrics and logs for most services in Azure. You can call Azure Automation runbooks by using action groups or by using classic alerts to automate tasks based on alerts.

Reference:

Question: 35

CertyIQ

HOTSPOT -

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.

Hot Area:

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: |
| readinessProbe: |
| ShutdownProbe: |
| startupProbe: |

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

| |
|-------------------------|
| initialDelaySeconds: 15 |
| periodSeconds: 15 |
| timeoutSeconds: 15 |

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:
        initialDelaySeconds: 15
        periodSeconds: 15
        timeoutSeconds: 15
      shutdownProbe:
```

Explanation:

Box1: shutdown probe

It clearly says "Initiate a shutdown if the pod is unresponsive."

How can you initiate a shutdown (restart) with readinessProbe.

It must have been livenessProbe.

Box 2: periodSeconds: 15 -

The periodSeconds property designates the readiness command should execute every 15 seconds.

Question: 36

CertyIQ

You have a Microsoft ASP.NET Core web app in Azure that is accessed worldwide.

You need to run a URL ping test once every five minutes and create an alert when the web app is unavailable from specific Azure regions. The solution must minimize development time.

What should you do?

- A. Create an Azure Monitor Availability metric and alert.
- B. Create an Azure Application Insights availability test and alert.**
- C. Write an Azure function and deploy the function to the specific regions.
- D. Create an Azure Service Health alert for the specific regions.

Answer: B

Explanation:

There are three types of Application Insights availability tests:

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

- ⇒ Multi-step web test
- ⇒ Custom Track Availability Tests

Note: After you've deployed your web app/website, you can set up recurring tests to monitor availability and responsiveness. Azure Application Insights sends web requests to your application at regular intervals from points around the world. It can alert you if your application isn't responding, or if it responds too slowly. You can set up availability tests for any HTTP or HTTPS endpoint that is accessible from the public internet. You don't have to make any changes to the website you're testing. In fact, it doesn't even have to be a site you own. You can test the availability of a REST API that your service depends on.

Reference:

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

Question: 37

CertyIQ

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. Azure Application Insights
- B. the activity log of the App Service
- C. the diagnostics logs of the App Service
- D. Azure Advisor

Answer: A

Explanation:

Application Insights will tell you about any performance issues and exceptions, and help you find and diagnose the root causes.

Application Insights can monitor both Java and ASP.NET web applications and services, WCF services. They can be hosted on-premises, on virtual machines, or as Microsoft Azure websites.

On the client side, Application Insights can take telemetry from web pages and a wide variety of devices including iOS, Android, and Windows Store apps.

Reference:

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

Question: 38

CertyIQ

SIMULATION -

You need to create an instance of Azure Application Insights named az400-123456789-main and configure the instance to receive telemetry data from an Azure web app named az400-123456789-main. To complete this task, sign in to the Microsoft Azure portal.

Answer:

See explanation 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.

New

Search the Marketplace

Azure Marketplace See all Featured See all

Get started DevOps Project Quickstart tutorial

Recently created DevTest Labs Quickstart tutorial

Compute Networking

Storage Web Chef Automate Learn more

Mobile Containers Application Insights Quickstart tutorial

Databases Analytics

AI + Machine Learning Internet of Things Jenkins Learn more

Mixed Reality Integration GitHub Enterprise Server Learn more

Security Identity Enterprise DC/OS on Azure Learn more

Developer Tools Management Tools Ansible Tower Learn more

Software as a Service (SaaS)

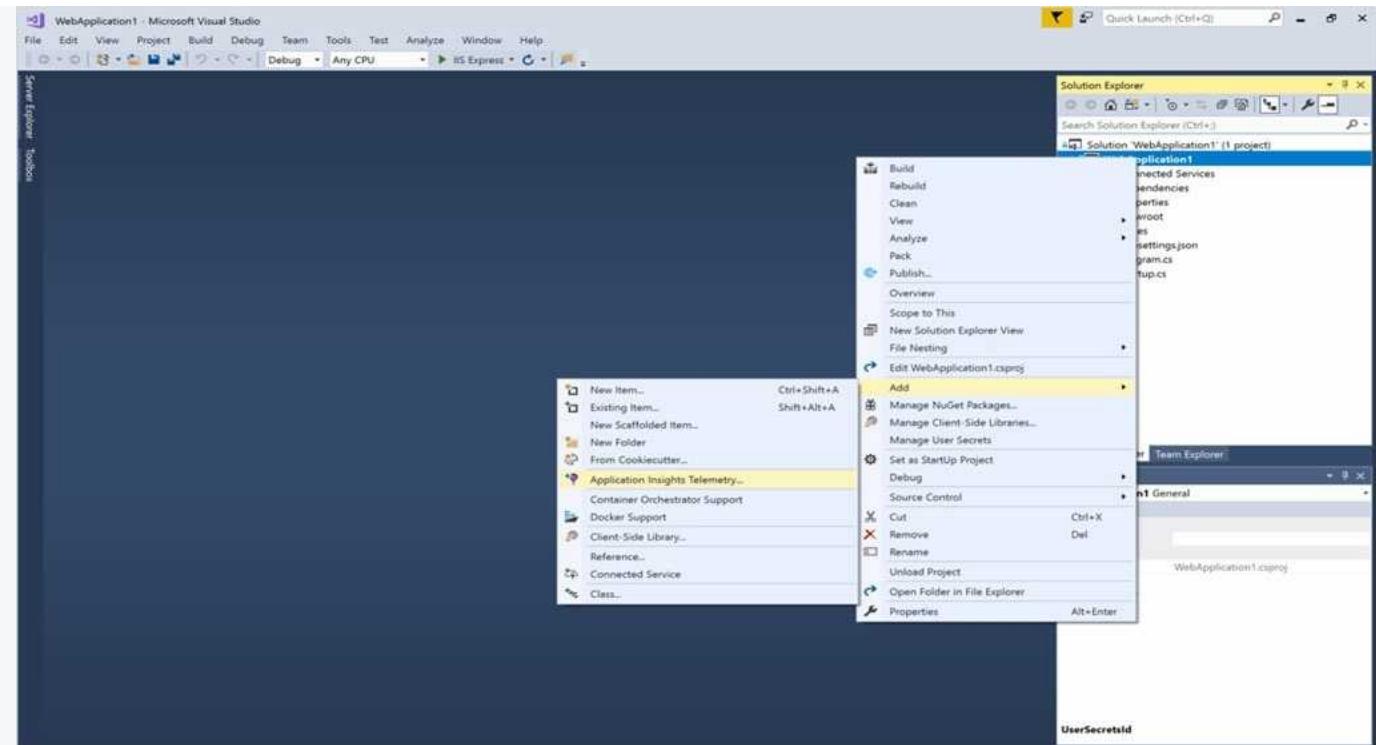
Blockchain

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

Name: az400-123456789-main -

Step 2: Configure App Insights SDK

1. 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.



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

Reference:

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

Question: 39

CertyIQ

Your company uses ServiceNow for incident management.

You develop an application that runs on Azure.

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

Which Azure Log Analytics solution should you use?

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

Answer: C

Explanation:

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

ITSMC supports connections with the following ITSM tools:

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

With ITSMC, you can -

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

Analytics workspace.

Reference:

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

Question: 40

CertyIQ

HOTSPOT -

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.

Hot Area:

Answer Area

Developers:

| |
|-------------|
| Basic |
| Stakeholder |

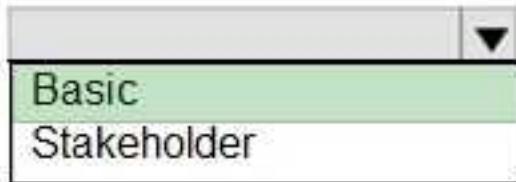
Pilot users:

| |
|-------------|
| Basic |
| Stakeholder |

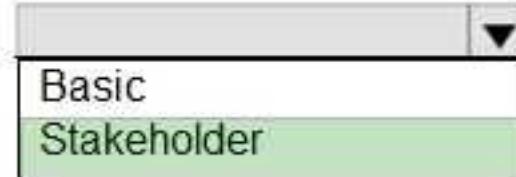
Answer:

Answer Area

Developers:



Pilot users:



Explanation:

Box 1: Basic -

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

Box 2: Stakeholder -

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

Note:

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

Basic: provides access to most features

VS Enterprise: provides access to premium features

Stakeholders: provides partial access, can be assigned to unlimited users for free

Reference:

<https://docs.microsoft.com/en-us/azure/devops/organizations/security/access-levels?view=vsts>

Question: 41

CertyIQ

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. Kusto Query Language (KQL)
- B. PL/pgSQL
- C. PL/SQL
- D. Transact-SQL

Answer: A

Explanation:

Azure Monitor Logs is based on Azure Data Explorer, and log queries are written using the same Kusto query language (KQL). This is a rich language designed to be easy to read and author, and you should be able to start using it with minimal guidance.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview>

CertyIQ

Question: 42

Your company creates a web application.

You need to recommend a solution that automatically sends to Microsoft Teams a daily summary of the exceptions that occur in the application.

Which two Azure services should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: AE

Explanation:

E: Exceptions in your live web app are reported by Application Insights.

Note: Periodical reports help keep a team informed on how their business critical services are doing.

Developers, DevOps/SRE teams, and their managers can be productive with automated reports reliably delivering insights without requiring everyone to sign in the portal. Such reports can also help identify gradual increases in latencies, load or failure rates that may not trigger any alert rules.

A: You can programmatically query Application Insights data to generate custom reports on a schedule. The following options can help you get started quickly:

- ⇒ Automate reports with Microsoft Flow
- ⇒ Automate reports with Logic Apps

Reference:

<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>

CertyIQ

Question: 43

DRAG DROP -

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

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

NOTE: Each correct selection is worth one point.

Select and Place:

Tools

Impact

User Flows

Users

Answer Area

Feature usage:

Number of people who used the actions and its features:

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:

Users

Number of people who used the actions and its features:

User Flows

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

Impact

Explanation:

Feature usage -> Users

User action by day -> User Flows

The effect ... -> Impact

Question: 44

CertyIQ

Your company is building a mobile app that targets Android and iOS devices.

Your team uses Azure DevOps to manage all work items and release cycles.

You need to recommend a solution to perform the following tasks:

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

What should you include in the recommendation?

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

Answer: B

Explanation:

For mobile, it is always Microsoft Visual Studio App Center

CertyIQ

Question: 45

You have an Azure DevOps project named Project1 and an Azure subscription named Sub1. Sub1 contains an Azure virtual machine scale set named VMSS1.

VMSS1 hosts a web application named WebApp1. WebApp1 uses stateful sessions.

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

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

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

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

NOTE: Each correct selection is worth one point.

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

Answer: CDE

Explanation:

Answer CDE

Not Correct:

A - State full sessions are already configured B - If you redeploy the VMSS1, the new configuration will apply to all virtual machines. "The requirement is: You need to implement limited user testing for the new version of WebApp1 on VMSS1."

CertyIQ

Question: 46

SIMULATION -

You need to create a notification if the peak average response time of an Azure web app named az400-123456789-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 explanation 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 -

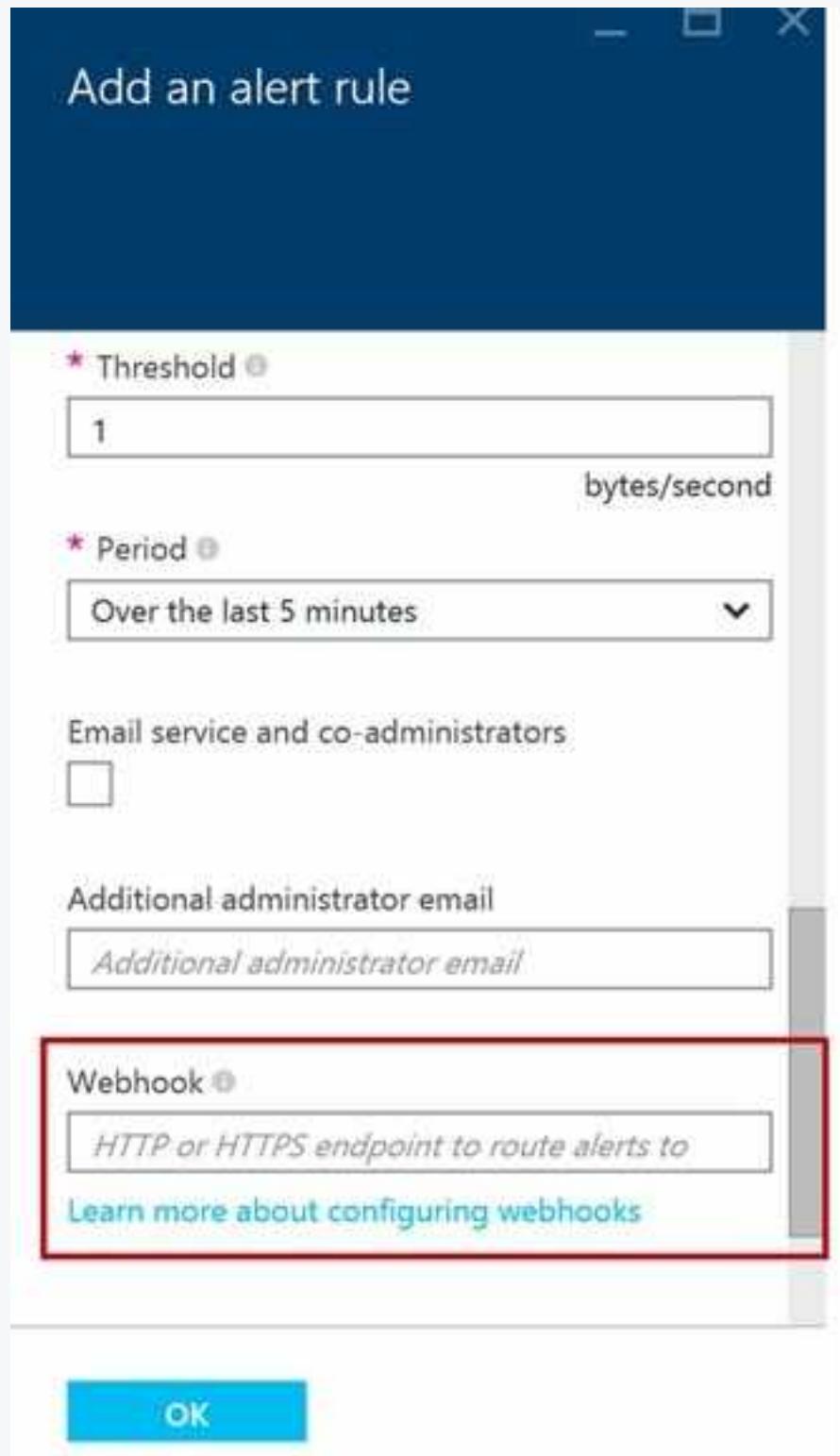
Resource Group: az400-123456789-main

Resource: az400-123456789-main -

Threshold: 5 -

Period: Over the last 5 minutes -

Webhook: <https://contoso.com/notify>



Reference:

Question: 47

SIMULATION -

You need to create and configure an Azure Storage account named az400lod123456789stor in a resource group named RG1lod123456789 to store the boot diagnostics for a virtual machine named VM1.

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

Answer:

See explanation below.

Explanation:

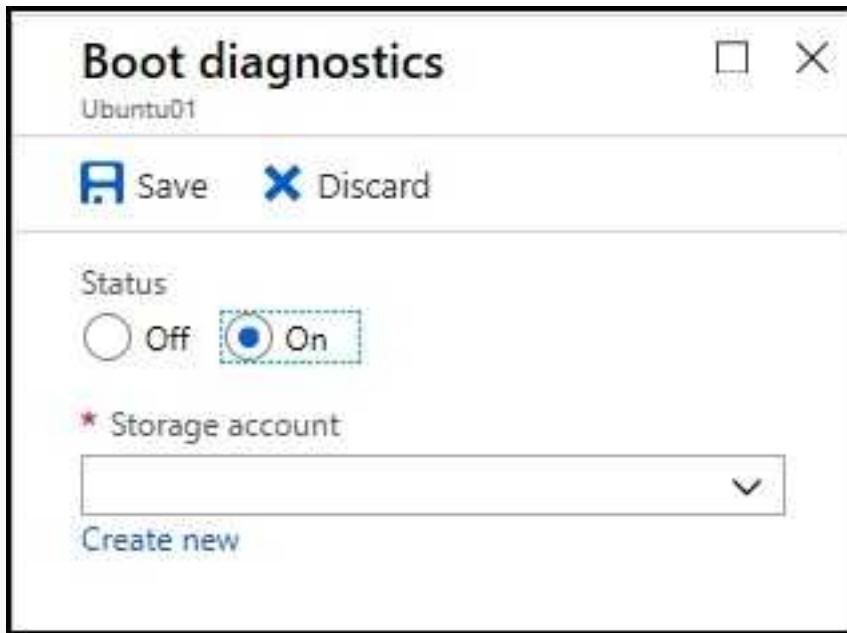
Step 1: To create a general-purpose v2 storage account in the Azure portal, follow these steps:

1. 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.
2. On the Storage Accounts window that appears, choose Add.
3. Select the subscription in which to create the storage account.
4. Under the Resource group field, select RG1lod123456789
5. Next, enter a name for your storage account named: az400lod123456789stor
6. 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 az400lod123456789stor.
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>

Question: 48

CertyIQ

SIMULATION -

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:

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.

The screenshot shows the Azure portal interface for managing diagnostic settings for a SQL database. The left sidebar contains a navigation menu with several sections: Connection strings, Sync to other databases, Add Azure Search, Properties, Locks, Automation script, Security (Advanced Threat Protection, Auditing, Dynamic Data Masking, Transparent data encryption), Intelligent Performance (Performance overview, Performance recommendations, Query Performance Insight, Automatic tuning), Monitoring (Alerts (Classic), Metrics, Diagnostic settings), Support + troubleshooting, and Resource health. The 'Diagnostic settings' option is highlighted with a red box. The main pane displays the current diagnostic configuration: Subscription is set to 'Workload Insight dev/test subscription', Resource group is 'widemo', and Resource type is '0 selected'. A prominent red box surrounds the 'Turn on diagnostics' button.

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

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-configure>

Question: 49

CertyIQ

DRAG DROP -

You have several Azure virtual machines that run Windows Server 2019.

You need to identify the distinct event IDs of each virtual machine as shown in the following table.

| Name | Event ID |
|------|--------------------------------|
| VM1 | [704, 701, 1501, 1500, 1085] |
| VM2 | [326, 105, 302, 301, 300, 102] |
| ... | ... |

How should you complete the Azure Monitor query? To answer, drag the appropriate values to the correct locations. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Values Answer Area

count()

Event

makelist(EventID)

| where TimeGenerated > ago(12h)

makeset(EventID)

| order by TimeGenerated desc

mv-expand

| [] [] by Computer

project

render

summarize

Answer:

Values**Answer Area**

| | |
|-------------------|--|
| count() | Event |
| makelist(EventID) | where TimeGenerated > ago(12h) |
| makeset(EventID) | order by TimeGenerated desc |
| mv-expand | <input type="checkbox"/> summarize <input type="checkbox"/> makeset(EventID) by Computer |
| project | |
| render | |
| summarize | |

Explanation:

You might find it useful to create a list only of distinct values. This list is called a set, and you can generate it by using the make set command:

Event

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

Question: 50**CertyIQ**

HOTSPOT -

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.

Hot Area:

Answer Area

```
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:

Answer Area

```
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:

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>

Question: 51

CertyIQ

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. custom events
- B. Application Insights Profiler
- C. usage analysis
- D. Smart Detection**
- E. Continuous export

Answer: D

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>

Question: 52

CertyIQ

HOTSPOT -

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.

Hot Area:

Answer Area

Azure pipelines

| |
|---------------|
| feedback |
| signin |
| subscribe |
| subscriptions |

| |
|---|
| https://dev.azure.com/contoso/contoso-app/ |
| https://dev.azure.com/contoso/contoso-app/_build |
| https://dev.azure.com/contoso/contoso-app/_packaging |
| https://dev.azure.com/contoso/contoso-app/_work-items |

Answer:

Answer Area

@azure pipelines

| |
|---------------|
| feedback |
| signin |
| subscribe |
| subscriptions |

| |
|---|
| https://dev.azure.com/contoso/contoso-app/ |
| https://dev.azure.com/contoso/contoso-app/_build |
| https://dev.azure.com/contoso/contoso-app/_packaging |
| https://dev.azure.com/contoso/contoso-app/_work-items |

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]

CertyIQ

Question: 53

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. Configure multi-factor authentication (MFA) for your GitHub account.
- B. Add the Azure Pipelines app to the GitHub repository.
- C. Add the Azure Boards app to the repository.**
- D. Create a GitHub action in GitHub.

Answer: C

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:

1. Sign into Azure Boards.
2. Choose (1) Project Settings, choose (2) GitHub connections and then (3) Connect your GitHub account.
3. 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.
4. 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 X

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>

Question: 54

CertyIQ

You are integrating Azure Pipelines and Microsoft Teams.

You install the Azure Pipelines app in Microsoft Teams.

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

You subscribe to Project1 in Microsoft Teams.

You need to ensure that you only receive events about failed builds in Microsoft Teams.

What should you do first?

- A. From Microsoft Teams, run @azure pipelines subscribe <https://dev.azure.com/Contoso/Project1>.
- B. From Azure Pipelines, add a Publish Build Artifacts task to Project1.
- C. From Microsoft Teams, run @azure pipelines subscriptions.**
- D. From Azure Pipelines, enable continuous integration for Project1.

Answer: C

Explanation:

Using filters effectively to customize subscriptions

When a user subscribes to any pipeline, a few subscriptions are created by default without any filters being applied. Often, users have the need to customize these subscriptions. For example, users may want to get notified only when builds fail or when deployments are pushed to a production environment. The Azure Pipelines app supports filters to customize what you see in your channel.

Run the @Azure Pipelines subscriptions command

Select View all subscriptions. In the list of subscriptions, if there is a subscription that is unwanted or should be modified (Example: creating noise in the channel), select Remove

Scroll down and select the Add subscription button

Select the required pipeline and the event

Select the appropriate filters and save

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

Question: 55

CertyIQ

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 the Microsoft Teams admin center, configure external access
- D. From Microsoft Teams, add a channel
- E. From Azure DevOps, install an extension

Answer: B

Explanation:

From Microsoft Teams, Configure a connector.

If you try from Azure DevOps, you getting the following message:

Subscriptions for this service are managed by the consumer service. To create a new subscription visit Microsoft T

Question: 56

CertyIQ

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

Create rule

Rules management



* RESOURCE

ASP-9bb7

Select

HIERARCHY

Contoso > CoreApp1



* CONDITION

Whenever the Activity Log has an event with Category='Administrative', Signal name='All Administrative operations', Status='failed'

Add

! Azure Alerts are currently limited to either 2 metric, 1 log, or 1 activity log signal per alert rule. To alert on more signals, please create additional alert rules.



ACTIONS GROUPS (optional)

Action group name

Contain actions

Application Insights Smart Detection

2 Email Azure Resource Manager Role(s)

Add

Create

! Action rules (preview) allows you to define actions at scale as well as suppress actions. Learn more about this functionality by clicking on this banner. [Learn more](#)

Which action will trigger an alert?

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

Answer: A

Explanation:

But Administrative it's Contains the record of all create, update, delete, and action operations performed through Resource Manager. So answer is A

Question: 57

CertyIQ

You have a web app hosted on Azure App Service. The web app stores data in an Azure SQL database. You need to generate an alert when there are 10,000 simultaneous connections to the database. The solution must minimize development effort.

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

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

Answer: A

Explanation:

ENABLE DIAGNOSTICS TO LOG ANALYTICS

This configuration is done PER DATABASE

1. Click on Diagnostics Settings and then Turn On Diagnostics

The screenshot shows the 'Diagnostic settings' page for the 'AdventureWorks (fonsecanet/AdventureWorks)' database. The left sidebar includes sections for Connection strings, Sync to other databases, Add Azure Search, Properties, Logins, 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 shows a 'Subscription' dropdown set to 'SEONSA Microsoft Azure Internal Consumption' and a 'Resource group' dropdown set to 'CSAAzureDB'. A list of metrics being collected is shown, including SQLInsights, Automat Tuning, QueryStoreRuntimeStatistics, QueryStoreWaitStatistics, Errors, DatabaseWaitStatistics, Timeouts, blocks, Deadlocks, Audit, SQLSecurityAuditEvents, and AllMetrics. The 'Metrics' link in the sidebar is also highlighted with a red box.

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

Diagnostics settings

Save Discard Delete

Name: Diagnostics

Archive to a storage account

Stream to an event hub

Send to Log Analytics

Subscription: SEFORSEC Microsoft Azure Internal Consumption

Log Analytics Workspace: forensicsAnalytics (westus) [westus]

Logs

SQLInsights

AutomaticTuning

QueryStoreRuntimeStatistics

QueryStoreWaitStatistics

Errors

DatabaseWaitStatistics

Timeouts

Blocks

Reference:
<https://techcommunity.microsoft.com/t5/azure-database-support-blog/azure-sql-db-and-log-analytics-better-together-part-1/ba-p/794833>

Question: 58

CertyIQ

HOTSPOT -

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.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Aggregation granularity (Period):

| |
|-----------|
| 1 minute |
| 5 minutes |

Threshold value:

| |
|---------|
| Static |
| Dynamic |

Operator:

| |
|--------------------------|
| Greater than |
| Greater than or equal to |
| Less than or equal to |
| Less than |

Answer:

Answer Area

Aggregation granularity (Period):

| |
|-----------|
| 1 minute |
| 5 minutes |

Threshold value:

| |
|---------|
| Static |
| Dynamic |

Operator:

| |
|--------------------------|
| Greater than |
| Greater than or equal to |
| Less than or equal to |
| Less than |

Explanation:

Box 1: 5 minutes -

The alert must calculate the average once every minute.

Note: We [Microsoft] recommend choosing an Aggregation granularity (Period) that is larger than the Frequency of evaluation, to reduce the likelihood of missing the first evaluation of added time series

Box 2: Static -

Box 3: Greater than -

Example, say you have an App Service plan for your website. You want to monitor CPU usage on multiple instances running your web site/app. You can do that using a metric alert rule as follows:

- ⇒ Target resource: myAppServicePlan
- ⇒ Metric: Percentage CPU
- ⇒ Condition Type: Static
- ⇒ Dimensions
- ⇒ Instance = InstanceName1, InstanceName2
- ⇒ Time Aggregation: Average
- ⇒ Period: Over the last 5 mins
- ⇒ Frequency: 1 min
- ⇒ Operator: GreaterThan
- ⇒ Threshold: 70
- ⇒ Like before, this rule monitors if the average CPU usage for the last 5 minutes exceeds 70%.
- ⇒ Aggregation granularity

Reference:

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

CertyIQ

Question: 59

You have an Azure virtual machine that is monitored by using Azure Monitor.

The virtual machine has the Azure Log Analytics agent installed.

You plan to deploy the Service Map solution from the Azure Marketplace.

What should you deploy to the virtual machine to support the Service Map solution?

- A. the Dependency agent
- B. the Telegraf agent
- C. the Windows Azure diagnostics extension (WAD)
- D. the Azure monitor agent

Answer: A

Explanation:

Use the Dependency agent if you need to use the Map feature VM insights or the Service Map solution.

Note: Consider the following when using the Dependency agent:

The Dependency agent requires the Log Analytics agent to be installed on the same machine.

On Linux computers, the Log Analytics agent must be installed before the Azure Diagnostic Extension.

On both the Windows and Linux versions of the Dependency Agent, data collection is done using a user-space service and a kernel driver.

Reference:

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

CertyIQ

Question: 60

HOTSPOT -

You have a project in Azure DevOps that contains a Continuous Integration/Continuous Deployment (CI/CD) pipeline.

You need to enable detailed logging by defining a pipeline variable.

How should you configure the variable? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Name:

| |
|--------------|
| Debug |
| Log |
| System.Debug |
| System.Log |

Value:

| |
|----------|
| 1 |
| detailed |
| true |

Answer:

Answer Area

Name:

Debug
Log
System.Debug
System.Log

Value:

1
detailed
true

Explanation:

Box 1: system.debug -

To configure verbose logs for all runs, you can add a variable named system.debug and set its value to true.

Note: Verbose logging is the practice of recording to a persistent medium as much information as you possibly can about events that occur while the software runs.

Box 2: true -

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/troubleshooting/review-logs>

Question: 61

CertyIQ

You build an iOS app.

You receive crash reports from Crashlytics.

You need to capture the following data:

- ⇒ Crash-free users
- ⇒ Custom events
- ⇒ Breadcrumbs

What should you do?

- A. Configure the xcworkspace file in the project
- B. Add the GoogleAnalytics pod to the app.
- C. Configure the Crashlytics pod in the app.

D. Import the Firebase module to UIApplicationDelegate.

Answer: D

Explanation:

Step 1: Add the Firebase Crashlytics SDK to your app.

Configure the Firebase module:

Import the Firebase module in your App struct or UIApplicationDelegate

Reference:

<https://firebase.google.com/docs/crashlytics/get-started?platform=ios>

CertyIQ

Question: 62

You have multiple teams that work on multiple projects in Azure DevOps.

You need to plan and manage the consumers and producers for each project. The solution must provide an overview of all the projects.

What should you do?

- A. Add a Predecessor or Successor link to the feature or user story for the items of each project.
- B. Add a Parent or Child link to the feature or user story for the items of each project.
- C. Install the Dependency Tracker extension and create dependencies for each project.**
- D. Create a custom query to show the consumers and producers and add a widget to a dashboard.

Answer: C

Explanation:

You use the Dependency Tracker to plan dependencies at the beginning of an iteration or release, and to track the status during development. For any given dependency, there are two parties involved:

Consumer: Feature team who has a need and starts a request for work

Producer: Feature team who makes a commitment to deliver work

<https://learn.microsoft.com/en-us/azure/devops/boards/extensions/dependency-tracker?view=azure-devops>

CertyIQ

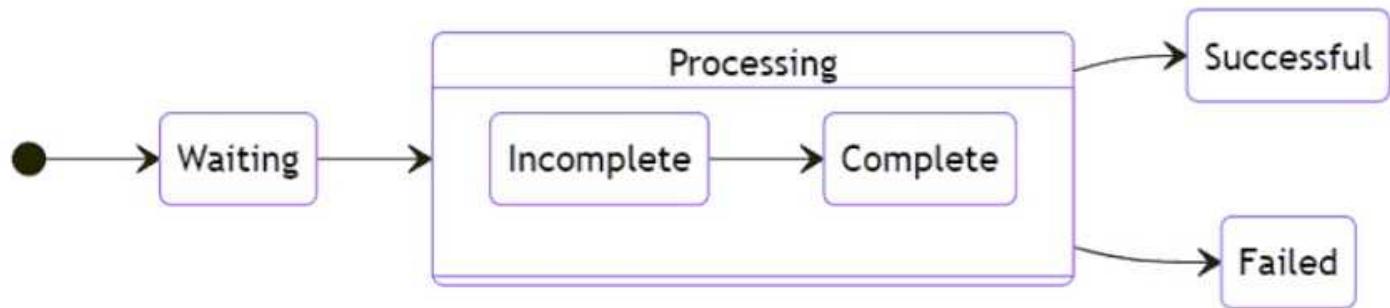
Question: 63

DRAG DROP

-

You have a GitHub repository that contains the source code for an app named App1.

You need to create process documentation for App1. The solution must include a diagram that displays the relationships between the phases of App1 as shown in the following exhibit.



How should you complete the markdown code? To answer, drag the appropriate values to the correct targets. 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

| |
|-----------------|
| Failed |
| flowChart |
| Incomplete |
| Processing |
| sequenceDiagram |
| stateDiagram |
| Waiting |

Answer Area

```

```mermaid
graph LR
 [*] --> Waiting
 Waiting --> Processing
 Processing --> Successful
 Processing --> Failed
 state {
 direction LR
 Incomplete --> Complete
 }
 Processing --> Failed
```

```

Answer:

Answer Area

```
```mermaid
```

```
stateDiagram
```

```
direction LR
```

```
[""] --> Waiting
```

```
Waiting --> Processing
```

```
Processing --> Successful
```

```
state Processing {
```

```
direction LR
```

```
Incomplete --> Complete
```

```
}
```

```
Processing --> Failed
```

```

```

CertyIQ

### Question: 64

HOTSPOT

You have an Azure web app named webapp1 that uses the .NET Core runtime stack. You have an Azure Application Insights resource named AppInsights1 that collects telemetry data generated by webapp1.

You plan to deploy webapp1 by using an Azure DevOps pipeline.

You need to modify the sampling rate of the telemetry data processed by AppInsights1 without having to redeploy webapp1 after each modification.

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

NOTE: Each correct selection is worth one point.

From the code repository of webapp1:

- Disable adaptive sampling.
- Enable fixed-rate sampling.
- Modify ApplicationInsights.config.

From AppInsights1:

- Configure Continuous export.
- Configure the Smart Detection settings.
- Modify the Usage and estimated costs settings.

**Answer:**

From the code repository of webapp1:

- Disable adaptive sampling.
- Enable fixed-rate sampling.
- Modify ApplicationInsights.config.**

From AppInsights1:

- Configure Continuous export.
- Configure the Smart Detection settings.
- Modify the Usage and estimated costs settings.**

**Question: 65**

CertyIQ

Your company has multiple microservices-based apps that use the following tracing libraries:

- OpenTelemetry
- OpenCensus
- OpenTracing
- Honeycomb
- Jaeger

The company purchases an Azure subscription and implements Application Insights in Azure Monitor.

You plan to centralize distributed tracing for the apps.

You need to identify which libraries can integrate directly with Application Insights.

Which two libraries should you identify? Each correct answer presents a complete solution.

NOTE: Each correct solution is worth one point.

- A. Honeycomb
- B. OpenTracing
- C. Jaeger
- D. OpenTelemetry**
- E. OpenCensus**

**Answer: DE**

**Explanation:**

Application Insights now supports distributed tracing through OpenTelemetry. OpenTelemetry provides a vendor-neutral instrumentation to send traces, metrics, and logs to Application Insights. Initially, the OpenTelemetry community took on distributed tracing.

In addition to the Application Insights SDKs, Application Insights also supports distributed tracing through OpenCensus. OpenCensus is an open-source, vendor-agnostic, single distribution of libraries to provide metrics collection and distributed tracing for services.

<https://learn.microsoft.com/en-us/azure/azure-monitor/app/distributed-tracing>

## Question: 66

CertyIQ

You have an Azure web app named webapp1 that uses the .NET Core runtime stack. You have an Azure Application Insights resource named Applnights1. Webapp1 sends telemetry data to Applnights1.

You need to ensure that webapp1 sends the telemetry data at a fixed sampling rate.

What should you do?

- A. From the code repository of webapp1, modify the ApplicationInsights.config file.
- B. From the code repository of webapp1, modify the Startup.cs file.
- C. From Applnights1, modify the Usage and estimated costs settings.
- D. From Applnights1, configure the Continuous export settings.

**Answer: B**

**Explanation:**

The question is not asking how you can change the rate at which Application Insights consumes the telemetry data - therefore, C and D cannot be correct. We are left with A and B as possible answers, but (as Azure Jobs Till Retire points out) answer A can't be correct, so B must be the correct answer.

## Question: 67

CertyIQ

DRAG DROP

You have an app named App1. You have a Log Analytics workspace named Workspace1 that contains two tables named Events and Logs. App1 manages events in multiple locations and writes logs to Workspace1.

You need to query Workspace1 for all log entries related to Asia that occurred during the last two days.

In which order should you arrange the query statements? To answer, move all statements from the list of statements to the answer area and arrange them in the correct order.

### Statements

### Answer Area

| where continent == 'Asia'

| join ( Events

Logs

| where timestamp > ago(2d)

) on RequestId



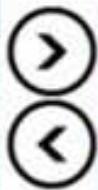
**Answer:**

## Statements

```
| where continent == 'Asia'
| join (Events
Logs
| where timestamp > ago(2d)
) on RequestId
```

## Answer Area

Logs



```
| where timestamp > ago(2d)
| join (Events
| where continent == 'Asia'
) on RequestId
```



### Explanation:

Logs

```
| where Timestamp > ago(2d)
```

```
| join
```

```
(
```

Events

```
| where continent == 'asia'
```

```
) on Request Id
```

<https://hybriddbablog.com/2022/03/31/kql-series-understanding-kql-queries-part-2/>

## Question: 68

CertyIQ

DRAG DROP

You have a web app named App1 that uses Application Insights in Azure Monitor.

You need to compare the hourly CPU usage of App1 from the last 24 hours. The solution must include a graph that has a threshold line at 75 percent.

How should you complete the query? To answer, drag the appropriate values to the correct targets. 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**

bin(TimeGenerated, 1d)  
bin(TimeGenerated, 1h)  
extend  
project  
render

**Answer Area**

```
...
performanceCounters
| where TimeGenerated > ago(1d)
| where counter == "% Processor Time"
| summarize avg(value) ,by cloud_RoleInstance,
| [REDACTED] Threshold = 75
```

**Answer:****Values**

bin(TimeGenerated, 1d)  
bin(TimeGenerated, 1h)  
extend  
project  
render

**Answer Area**

```
...
performanceCounters
| where TimeGenerated > ago(1d)
| where counter == "% Processor Time"
| summarize avg(value) ,by cloud_RoleInstance,
| render [REDACTED] Threshold = 75
```

**Explanation:**

performance counters| where TimeGenerated > ago(1d)| where counter == "% Processor Time"| summarize avg(value), by cloud\_RoleInstance, bin(TimeGenerated, 1d)| render Threshold = 75

**Question: 69****CertyIQ**

You use Azure Pipelines to build and deploy an app named App1.

You plan to monitor App1 by using Application Insights.

You create an Application Insights instance named AI1.

You need to configure App1 to use AI1.

Which file should you modify?

- A.appsettings.json
- B.launchSettings.json
- C.Startup.cs**
- D.project.json

**Answer: C****Explanation:**

Answer:C. startup.csIn a typical .NET application, such as App1, the startup.cs file contains the configuration and initialization code for the application. This file is responsible for configuring various services and middleware during the application's startup. To enable and configure Application Insights, you would modify the startup.cs file and add the necessary code to set up Application Insights for your app. This typically

involves adding services and configuring the Application Insights instrumentation key, which connects your app to the AI1 instance.

## Question: 70

CertyIQ

HOTSPOT

You have an Azure virtual machine named web1.

You need to query the amount of free memory that was available on web1 during the past seven days. The solution must meet the following requirements:

- Display the data as a time chart.
- Calculate the average value per hour.

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

NOTE: Each correct selection is worth one point.

### Answer Area

```
...
| where Computer == "web1"
| where CounterName == "Available MBytes"
| summarize avg(CounterValue) by
| render timechart
...
| where TimeGenerated > ago(7d)
| where TimeGenerated < ago(7d)
| where TimeGenerated == ago(7d)
```

bin(TimeGenerated, 1d)  
bin(TimeGenerated, 1h)  
dcount(CounterName)

Answer:

## Answer Area

```
...
Perf
| where
 TimeGenerated > ago(7d)
 TimeGenerated < ago(7d)
 TimeGenerated == ago(7d)
| where Computer == "web1"
| where CounterName == "Available MBytes"
| summarize avg(CounterValue) by
| render timechart
 bin(TimeGenerated, 1d)
 bin(TimeGenerated, 1h)
 dcount(CounterName)
...
```

### Explanation:

1. TimeGenerated > ago (7d)
2. bin(TimeGenerated, 1h)

<https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/agofunction> Subtracts the given timespan from the current UTC time.  
<https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/binfunction> Rounds values down to an integer multiple of a given bin size.

## Question: 71

CertyIQ

You have an Azure subscription that contains multiple Azure services.  
You need to send an SMS alert when scheduled maintenance is planned for the Azure services.  
Which two actions should you perform? Each correct answer presents part of the solution.  
NOTE: Each correct selection is worth one point.

- A. Enable Azure Security Center.
- B. Create and configure an Azure Monitor alert rule.
- C. **Create an Azure Service Health alert.**
- D. Create and configure an action group.

### Answer: CD

### Explanation:

Creating planned maintenance alerts using Azure Service Health

1. Login into the Azure portal and select Service Health.
  2. Select Health alerts followed by + Create service health alert from the top of the window on the right.
  3. In the Edit Alert blade, give the alert a Name, Description, check the subscription is correct and choose a resource group.
  4. The next step is to work through the Criteria section choosing which services, regions and types of event alerts should be monitored. For the purpose of this article all services and regions have been checked but only planned maintenance events.
  5. Select or create an Action group. (An Action group is a group of actions to be taken, should an event be logged.)
  6. Configure the actions to be taken. We are only configuring an email alert, so we first name the action, then chose Email/SMS/Push/Voice from the drop down list.
- Note: Azure Service Health can be used to view problems with Azure services that may impact any of your

cloud services. Service Health monitors three types of health event:  
Service issues " Azure services that are currently experiencing problems  
Planned maintenance " Any known future maintenance that may affect the availability of your services  
Health advisories " Changes in services, for example, deprecated features or exceeded quota usage.

Reference:

<https://www.techkb.onl/azure-using-service-health-to-alert-against-planned-maintenance/>

CertyIQ

## Question: 72

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 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, configure the autoscale settings.

Does this meet the goal?

- A. Yes
- B. No

## Answer: B

### Explanation:

Instead create an action group.

Note: An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor, Service Health and Azure Advisor alerts use action groups to notify users that an alert has been triggered.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups>

CertyIQ

## Question: 73

You configure Azure Application Insights and the shared service plan tier for a web app.

You enable Smart Detection.

You confirm that standard metrics are visible in the logs, but when you test a failure, you do not receive a Smart Detection notification.

What prevents the Smart Detection notification from being sent?

- A. You must enable the Snapshot Debugger for the web app.
- B. Smart Detection uses the first 24 hours to establish the normal behavior of the web app.
- C. The web app is configured to use the shared service plan tier.
- D. You must restart the web app before Smart Detection is enabled.

## Answer: B

**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>

**CertyIQ****Question: 74**

DRAG DROP -

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 processes 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.

Select and Place:

**Processes**

Agile

CMMI

Scrum

XP

**Answer Area**

Litware

Contoso:

A. Datum:

**Answer:**

## Processes

Agile

CMMI

Scrum

XP

## Answer Area

Litware

Scrum

Contoso:

Agile

A. Datum:

CMMI

### Explanation:

Box 1: Scrum -

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

Box 2: Agile -

Choose Agile when your team uses Agile planning methods, including Scrum, and tracks development and test activities separately. This process works great if you want to track user stories and (optionally) bugs on the Kanban board, or track bugs and tasks on the taskboard.

Box 3: CMMI -

Choose CMMI when your team follows more formal project methods that require a framework for process improvement and an auditable record of decisions. With this process, you can track requirements, change requests, risks, and reviews.

Incorrect Answers:

XP:

The work tracking objects contained within the default DevOps processes and DevOps process templates are Basic, Agile, CMMI, and Scrum

XP (Extreme Programming) and DevOps are different things. They don't contradict with each other, they can be used together, but they have different base concepts inside them.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/boards/work-items/guidance/choose-process?view=azure-devops>

## Question: 75

CertyIQ

You configure an Azure Application Insights availability test.

You need to notify the customer services department at your company by email when availability is degraded.

You create an Azure logic app that will handle the email and follow up actions.

Which type of trigger should you use to invoke the logic app?

- A. an HTTPWebhook trigger
- B. an HTTP trigger
- C. a Request trigger
- D. an ApiConnection trigger

**Answer: B**

**Explanation:**

HTTP trigger

<https://docs.microsoft.com/en-us/azure/app-service/tutorial-send-email?tabs=dotnet>

CertyIQ

**Question: 76**

You have an Azure DevOps organization named Contoso and an Azure subscription.

You use Azure DevOps to build a containerized app named App1 and deploy App1 to an Azure container instance named ACI1.

You need to restart ACI1 when App1 stops responding.

What should you do?

- A. Add a liveness probe to the YAML configuration of App1.
- B. Add a readiness probe to the YAML configuration of App1.
- C. Use Connection Monitor in Azure Network Watcher.
- D. Use IP flow verify in Azure Network Watcher.

**Answer: A**

**Explanation:**

Liveness Probe

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

CertyIQ

**Question: 77**

You have a multi-tier application that has an Azure Web Apps front end and an Azure SQL Database back end. You need to recommend a solution to capture and store telemetry data. The solution must meet the following requirements:

- ⇒ Support using ad-hoc queries to identify baselines.
- ⇒ Trigger alerts when metrics in the baseline are exceeded.
- ⇒ Store application and database metrics in a central location.

What should you include in the recommendation?

- A. Azure Event Hubs
- B. Azure SQL Database Intelligent Insights
- C. Azure Application Insights
- D. Azure Log Analytics

**Answer: D**

**Explanation:**

Azure Platform as a Service (PaaS) resources, like Azure SQL and Web Sites (Web Apps), can emit performance metrics data natively to Log Analytics.

The Premium plan will retain up to 12 months of data, giving you an excellent baseline ability.

There are two options available in the Azure portal for analyzing data stored in Log analytics and for creating queries for ad hoc analysis.

**Incorrect Answers:**

B: Intelligent Insights analyzes database performance by comparing the database workload from the last hour with the past seven-day baseline workload.

However, we need handle application metrics as well.

**Reference:**

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-azurepass-posh>

**Question: 78****CertyIQ**

You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 that is configured for autoscaling.

You use Azure DevOps to build a web app named App1 and deploy App1 to VMSS1. App1 is used heavily and has usage patterns that vary on a weekly basis.

You need to recommend a solution to detect an abnormal rise in the rate of failed requests to App1. The solution must minimize administrative effort.

What should you include in the recommendation?

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

**Answer: A****Explanation:**

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

**Reference:**

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

**Question: 79****CertyIQ****SIMULATION -**

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 explanation below.

**Explanation:**

Enable Remote Debugging -

Before we start a debugging session to our Azure Function app we need to enable the functionality.

1. Navigate in the Azure portal to your function app fa-11566895
2. Go to the Application settings
3. 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/>

## Question: 80

CertyIQ

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

**Answer: D**

**Explanation:**

Azure Dashboards

<https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-dashboards>

## Question: 81

CertyIQ

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.

Reference:

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

## Question: 82

CertyIQ

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 <InitialSamplingPercentage>99</InitialSamplingPercentage> parameter to the ApplicationInsights.config file.
- B. From the code of the application, enable adaptive sampling.
- C. **From the code of the application, add Azure Application Insights telemetry.**
- D. Add the <MaxTelemetryItemsPerSecond>5</MaxTelemetryItemsPerSecond> parameter to the ApplicationInsights.config file.
- E. **From the code of the application, disable adaptive sampling.**

**Answer: CE**

**Explanation:**

Disable Adaptive Sampling and use Fixed Rate Sampling instead:

"Fixed-rate sampling reduces the volume of telemetry sent from both your ASP.NET or ASP.NET Core or Java server and from your users' browsers. You set the rate. The client and server will synchronize their sampling so that, in Search, you can navigate between related page views and requests."

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

## Question: 83

**CertyIQ**

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. an Azure Load Balancer health probe
- B. Azure Monitor autoscale
- C. the Custom Script Extension
- D. the Application Health extension**

**Answer: D**

**Explanation:**

Monitoring your application health is an important signal for managing and upgrading your deployment. Azure virtual machine scale sets provide support for rolling upgrades including automatic OS-image upgrades, which rely on health monitoring of the individual instances to upgrade your deployment. You can also use health extension to monitor the application health of each instance in your scale set and perform instance repairs using automatic instance repairs.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-health-extensi>

**Question: 84**

HOTSPOT -

You have an application named App1 that has a custom domain of app.contoso.com. You create a test in Azure Application Insights as shown in the following exhibit.

## Create test

### Basic Information

\* Test name

availability

[Learn more about configuring tests against applications hosted behind a firewall](#)

Test type

URL ping test



\* URL

https://app.contoso.com



Parse dependent requests



Enable retries for availability test failures.



Test frequency

5 minutes



### Test locations

4 location(s) configured

### Success criteria

Test Timeout

30 seconds

 HTTP response

Status code must equal

200

 Content match

Content must contain

▼ 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.

Hot Area:

**Answer Area**

The test will execute [answer choice].

|                                         |
|-----------------------------------------|
| every 30 seconds at a random location   |
| every 30 seconds per location           |
| every five minutes at a random location |
| every five minutes per location         |

The test will pass if [answer choice] within 30 seconds.

|                                                          |
|----------------------------------------------------------|
| App1 responds to an ICMP ping                            |
| the HTML of App1 and the HTML from URLs in <a> tags load |
| all the HTML, JavaScripts, and images of App1 load       |

**Answer:**

**Answer Area**

The test will execute [answer choice].

|                                         |
|-----------------------------------------|
| every 30 seconds at a random location   |
| every 30 seconds per location           |
| every five minutes at a random location |
| every five minutes per location         |

The test will pass if [answer choice] within 30 seconds.

|                                                          |
|----------------------------------------------------------|
| App1 responds to an ICMP ping                            |
| the HTML of App1 and the HTML from URLs in <a> tags load |
| all the HTML, JavaScripts, and images of App1 load       |

**Explanation:**

Box1: every five minutes per location

I tested this in my lab and confirmed that each location will be tested every minute.

Box2: All the HTML, JavaScripts, and images of App1 load

If you selected Parse dependent requests, then all the images, style files, scripts, and other dependent resources must have been received within this period.

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

CertyIQ

### Question: 85

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

### Answer: BD

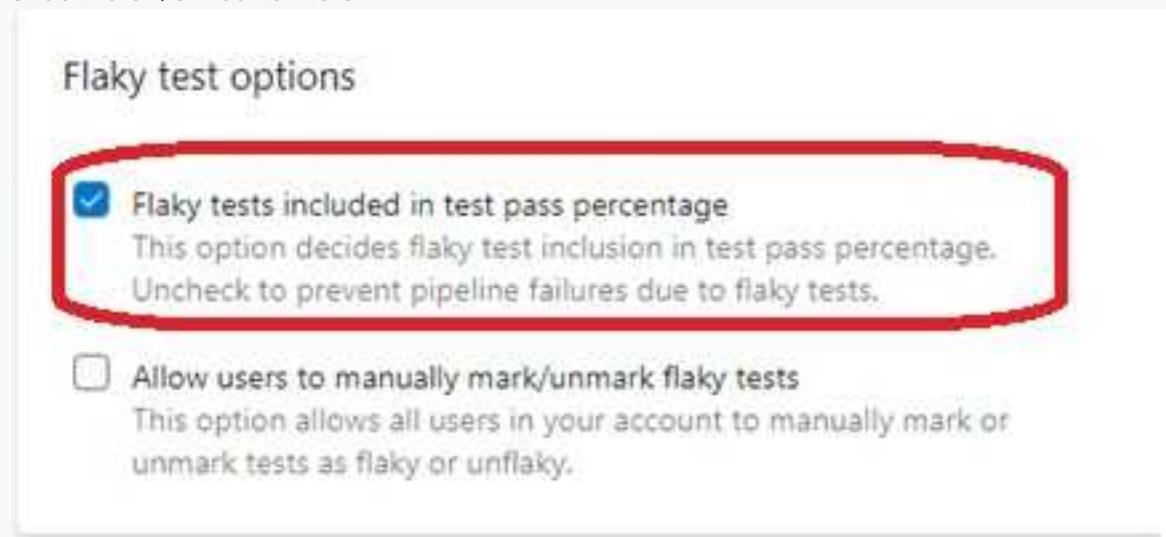
#### Explanation:

D: You can mark or unmark a test as flaky based on analysis or context, by choosing Flaky.

To configure flaky test management, choose Project settings, and select Test management in the Pipelines section.

B:

Slide the On/Off button to On.



Reference:

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

CertyIQ

### Question: 86

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.

Reference:

<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>

**Question: 87**

**CertyIQ**

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>

## Question: 88

CertyIQ

Your company uses the following resources:

- ⇒ Windows Server 2019 container images hosted in an Azure Container Registry.
- ⇒ Azure virtual machines that run the latest version of Ubuntu
- ⇒ An Azure Log Analytics workspace
- ⇒ Azure Active Directory (Azure AD)
- ⇒ An Azure key vault

For which two resources can you receive vulnerability assessments in Azure Security Center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the Azure Log Analytics workspace
- B. the Azure key vault
- C. the Azure virtual machines that run the latest version of Ubuntu**
- D. Azure Active Directory (Azure AD)
- E. The Windows Server 2019 container images hosted in the Azure Container Registry.**

**Answer: CE**

**Explanation:**

"Follow recommendations from Azure Security Center on performing vulnerability assessments on your Azure virtual machines, container images, and SQL servers."

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-control-vulnerability-management>

## Question: 89

CertyIQ

You use Azure Pipelines to manage build pipelines, GitHub to store source code, and Dependabot to manage dependencies.

You have an app named App1.

Dependabot detects a dependency in App1 that requires an update.

What should you do first to apply the update?

- A. Create a pull request.
- B. Approve the pull request.**
- C. Create a branch.
- D. Perform a commit.

**Answer: B**

**Explanation:**

DependaBot is a useful tool to regularly check for dependency updates. By helping to keep your project up to date, DependaBot can reduce technical debt and immediately apply security vulnerabilities when patches are released. How does DependaBot work?

1. DependaBot regularly checks dependencies for updates
2. If an update is found, DependaBot creates a new branch with this upgrade and Pull Request for approval
3. You review the new Pull Request, ensure the tests passed, review the code, and decide if you can merge the change

Reference:

<https://samlearnsazure.blog/2019/12/20/github-using-dependabot/>

## Question: 90

CertyIQ

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>

## Question: 91

CertyIQ

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-Continous-Assurance/Readme.html>

## Question: 92

CertyIQ

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>

CertyIQ

### Question: 93

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) permissions
- ⇒ 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>

## Question: 94

CertyIQ

You have a containerized solution that runs in Azure Container Instances. The solution contains a frontend container named App1 and a backend container named DB1. DB1 loads a large amount of data during startup. You need to verify that DB1 can handle incoming requests before users can submit requests to App1. What should you configure?

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

### Answer: C

#### Explanation:

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

Incorrect Answers:

A: Containerized applications may run for extended periods of time, resulting in broken states that may need to be repaired by restarting the container. Azure Container Instances supports liveness probes so that you can configure your containers within your container group to restart if critical functionality is not working.

Reference:

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

## Question: 95

CertyIQ

You are designing a strategy to monitor the baseline metrics of Azure virtual machines that run Windows Server. You need to collect detailed data about the processes running in the guest operating system. Which two agents should you deploy? Each correct answer presents part of the solution.  
NOTE: Each correct selection is worth one point.

- A. the Telegraf agent**
- B. the Azure Log Analytics agent**
- C. the Azure Network Watcher Agent for Windows
- D. the Dependency agent

### Answer: BD

### Explanation:

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

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

### Question: 96

CertyIQ

DRAG DROP -

You use Azure Pipelines to automate Continuous Integration/Continuous Deployment (CI/CD) for an Azure web app named WebApp1.

You configure an Azure Monitor alert that is triggered when WebApp1 generates an error.

You need to configure the alert to forward details of the error to a third-party system. The solution must minimize administrative effort.

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

Select and Place:

## Actions

## Answer Area

Select the Recurrence trigger.

Create an Azure event hub.

Create an Azure logic app.

Select the HTTP request trigger.

Update the action group in Azure Monitor.

Select the Sliding Window trigger.



Answer:

## Actions

## Answer Area

Select the Recurrence trigger.

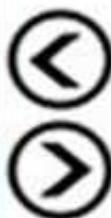
Create an Azure event hub.

Select the Sliding Window trigger.

Create an Azure logic app.

Select the HTTP request trigger.

Update the action group in Azure Monitor.



### Explanation:

Box 1: Create an Azure logic app.

Box 2: Select the HTTP request trigger.

Box 3: Updated the action group in Azure Monitor.

### Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups-logic-app>

## Question: 97

CertyIQ

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 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: B****Explanation:**

Notifications help you and your team stay informed about activity that occurs within your projects in Azure DevOps. You can get notified when changes occur to the following items:

- ⇒ work items
- ⇒ code reviews
- ⇒ pull requests
- ⇒ source control files
- builds

Reference:

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

**Question: 98****CertyIQ**

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 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 Service hooks settings for Project1.

Does this meet the goal?

A. Yes

B. No

**Answer: B****Question: 99****CertyIQ**

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 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: A****Explanation:**

An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor, Service Health and Azure Advisor alerts use action groups to notify users that an alert has been triggered.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups>

CertyIQ

### Question: 100

DRAG DROP -

You are using the Dependency Tracker extension in a project in Azure DevOps.

You generate a risk graph for the project.

What should you use in the risk graph to identify the number of dependencies and the risk level of the project? To answer, drag the appropriate elements to the correct data points. Each element may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

#### Elements

Link color

Link length

Link width

Node color

#### Answer Area

Number of dependencies

Risk level

Answer:

#### Elements

Link color

Link length

Link width

Node color

#### Answer Area

Number of dependencies

Risk level

Link width

Link color

#### Explanation:

Box 1: Link width -

The width of the lines indicates how many dependencies exist in that area, the thicker the link the more dependencies as indicated in the legend.

Box 2: Link color -

Reference:

<https://docs.microsoft.com/en-us/azure/devops/boards/extensions/dependency-tracker?view=azure-devops#risk-graph>

CertyIQ

### Question: 101

You have an Azure subscription linked to an Azure Active Directory Premium Plan 1 tenant.

A security review indicates that too many users have privileged access to resources.

You need to deploy a privileged access management solution that meets the following requirements:

- Enforces time limits on the use of privileged access
- Requires approval to activate privileged access
- Minimizes costs

What should you do first?

- A. Configure notifications when privileged roles are activated.
- B. Configure alerts for the activation of privileged roles.
- C. Enforce Azure Multi-Factor Authentication (MFA) for role activation.
- D. Upgrade the license of the Azure Active Directory (Azure AD) tenant.

Answer: D

Explanation:

Using Azure AD Privileged Identity Management (PIM) requires Azure AD Premium P2 licenses.

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

CertyIQ

### Question: 102

You have a GitHub Enterprise account.

You need to enable push protection for secret scanning of the account repositories.

What should you do first?

- A. Purchase a GitHub Advanced Security license.
- B. Purchase Premium Plus support.
- C. Enforce multi-factor authentication (MFA).
- D. Create an access policy for secrets.

Answer: A

Explanation:

Secret scanning alerts for partners run automatically on all public repositories. If you have a license for GitHub Advanced Security, you can enable and configure secret scanning alerts for users for any repository owned by an organization.

[https://docs.github.com/en/\[email protected\]/code-security/secret-scanning/protecting-pushes-with-secret-scanning](https://docs.github.com/en/[email protected]/code-security/secret-scanning/protecting-pushes-with-secret-scanning)

**Question: 103**

CertyIQ

DRAG DROP -

Your company has a project in Azure DevOps named Project1.

All the developers at the company have Windows 10 devices.

You need to create a Git repository for Project1. The solution must meet the following requirements:

- Support large binary files.
- Store binary files outside of the repository.
- Use a standard Git workflow to maintain the metadata of the binary files by using commits to the repository.

Which three actions should you perform in sequence on each developer's device? 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**

Configure SSH key-based authentication.

Configure personal access token (PAT)-based authentication.

Perform a custom installation of Git for Windows that includes Git Virtual File System (GVFS).

Configure Git Large File Storage (LFS) file tracking.

Perform a custom installation of Git for Windows that includes Git Large File Storage (LFS).

**Answer:****Actions****Answer Area**

Configure SSH key-based authentication.

Configure personal access token (PAT)-based authentication.

Configure personal access token (PAT)-based authentication.

Perform a custom installation of Git for Windows that includes Git Large File Storage (LFS).

Perform a custom installation of Git for Windows that includes Git Virtual File System (GVFS).



Configure Git Large File Storage (LFS) file tracking.

Configure Git Large File Storage (LFS) file tracking.

Perform a custom installation of Git for Windows that includes Git Large File Storage (LFS).

**Explanation:**

Configure PAT

Perform installation of Git LFS

Track GIT LFS

<https://docs.github.com/en/repositories/working-with-files/managing-large-files/about-git-large-file-storage>

CertyIQ

### Question: 104

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/>

CertyIQ

### Question: 105

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. xCODE

### 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.

Reference:

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

CertyIQ

### Question: 106

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

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

What should you use?

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

### Answer: C

#### Explanation:

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

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

Azure DevOps integration with WhiteSource Bolt will enable you to:

1. Detect and remedy vulnerable open source components.
2. Generate comprehensive open source inventory reports per project or build.
3. Enforce open source license compliance, including dependencies' licenses.
4. Identify outdated open source libraries with recommendations to update.

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

Reference:

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

CertyIQ

### Question: 107

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

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

What should you use?

- A. Microsoft Visual SourceSafe
- B. Code Style
- C. Black Duck**
- D. Jenkins
- E. SourceGear
- F. OWASP ZAP

### Answer: C

**Explanation:**

Secure and Manage Open Source Software

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

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

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

Reference:

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

**CertyIQ****Question: 108**

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>

**CertyIQ****Question: 109**

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 an open source platform for continuous inspection of code quality to perform automatic reviews with static analysis of code to:

- ⇒ Detect Bugs
- ⇒ Code Smells
- ⇒ Security Vulnerabilities

Centralize Quality -

- ⇒ What's covered in this lab

Reference:

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

[Implement Continuous Delivery](#)

CertyIQ

### Question: 110

HOTSPOT -

You have an Azure subscription that contains the resources shown in the following table.

| Name | Type               |
|------|--------------------|
| DF1  | Azure Data Factory |
| SQL1 | Azure SQL Database |
| KV1  | Azure Key Vault    |

You plan to create a linked service in DF1. The linked service will connect to SQL1 by using Microsoft SQL Server authentication. The password for the SQL

Server login will be stored -  
in KV1.

You need to configure DF1 to retrieve the password when the data factory connects to SQL1. The solution must use the principle of least privilege.

How should you configure DF1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Permission type:

|             |
|-------------|
| Key         |
| Secret      |
| Certificate |

Access method:

|                                  |
|----------------------------------|
| Access policy                    |
| Service endpoint policy          |
| Role-based access control (RBAC) |

Answer:

## Answer Area

Permission type:

|             |
|-------------|
| Key         |
| Secret      |
| Certificate |

Access method:

|                                  |
|----------------------------------|
| Access policy                    |
| Service endpoint policy          |
| Role-based access control (RBAC) |

### Explanation:

Box 1: Secret -

Store credential in Azure Key Vault by reference secret stored in key vault.

To reference a credential stored in Azure Key Vault, you need to:

1. Retrieve data factory managed identity
2. Grant the managed identity access to your Azure Key Vault. In your key vault -> Access policies -> Add Access Policy, search this managed identity to grant

Get permission in Secret permissions dropdown. It allows this designated factory to access secret in key vault.

3. Create a linked service pointing to your Azure Key Vault.
4. Create data store linked service, inside which reference the corresponding secret stored in key vault.

Box 2: Access policy -

Reference:

<https://docs.microsoft.com/en-us/azure/data-factory/store-credentials-in-key-vault>

### Question: 111

CertyIQ

You have several Azure Active Directory (Azure AD) accounts.  
You need to ensure that users use multi-factor authentication (MFA) to access Azure apps from untrusted networks.  
What should you configure in Azure AD?

- A. access reviews
- B. managed identities
- C. entitlement management
- D. conditional access

Answer: D

Explanation:

You can configure a Conditional Access policy that requires MFA for access from untrusted networks.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa>

### Question: 112

CertyIQ

You plan to provision a self-hosted Linux agent.  
Which authentication mechanism should you use to register the self-hosted agent?

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

Answer: A

Explanation:

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

Reference:

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

### Question: 113

CertyIQ

You are building a Microsoft ASP.NET application that requires authentication. You need to authenticate users by using Azure Active Directory (Azure AD). What should you do first?

- A. Assign an enterprise application to users and groups
- B. Create an app registration in Azure AD**
- C. Configure the application to use a SAML endpoint
- D. Create a new OAuth token from the application
- E. Create a membership database in an Azure SQL database

#### Answer: B

#### Explanation:

Register your application to use Azure Active Directory. Registering the application means that your developers can use Azure AD to authenticate users and request access to user resources such as email, calendar, and documents.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/developer-guidance-for-integrating-applications>

### Question: 114

CertyIQ

You have an Azure DevOps organization named Contoso.

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

- ⇒ Supports authentication from Git
- ⇒ Minimizes the need to provide credentials during authentication

What should you recommend?

- A. personal access tokens (PATs) in Azure DevOps**
- B. Alternate credentials in Azure DevOps
- C. user accounts in Azure Active Directory (Azure AD)
- D. managed identities in Azure Active Directory (Azure AD)

#### Answer: A

#### 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.

Incorrect Answers:

B: Azure DevOps no longer supports Alternate Credentials authentication since the beginning of March 2, 2020. If you're still using Alternate Credentials, we [Microsoft] strongly encourage you to switch to a more secure authentication method (for example, personal access tokens).

Reference:

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

**Question: 115**

CertyIQ

You have an application that consists of several Azure App Service web apps and Azure functions.

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

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

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

**Answer: D****Explanation:**

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

Recommendations -

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

Incorrect Answers:

C: Smart Detection automatically warns you of potential performance problems, not security problems in your web application.

Reference:

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

**Question: 116**

CertyIQ

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 an Azure Key Vault task to the pipeline.
- D. Add Azure Key Vault references to Azure Resource Manager templates.**

**Answer: D****Explanation:**

D is correct and needed, so the correct answer BE D because the requirement is to minimize the likelihood that infrastructure credentials will be leaked. The security is one of the highest priority, and for that the possibility to know the secret name (as AKV task could consent) is not the best practice.

**Question: 117**

CertyIQ

SIMULATION -

You need to ensure that an Azure web app named az400-123456789-main can retrieve secrets from an Azure key vault named az400-123456789-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 explanation below.

#### Explanation:

1. In Azure portal navigate to the az400-123456789-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.

The screenshot shows the Azure portal interface for managing identities. The left sidebar has a 'Settings' group expanded, with 'Identity' selected. The main content area is titled 'systemassigned-linux - Identity' and shows the 'System assigned' tab selected under 'Identity'. A status bar at the bottom indicates the resource is registered with Azure Active Directory. The 'Status' button is set to 'On'.

#### Reference:

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

### Question: 118

CertyIQ

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>

CertyIQ

### Question: 119

DRAG DROP -

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.

Select and Place:

#### Configurations

A Key Vault access policy

A Key Vault advanced access policy

RBAC

#### Answer Area

Enable key vaults for template deployment by using:

Restrict access to the secrets in Key Vault by using:

### Answer:

#### Configurations

A Key Vault access policy

A Key Vault advanced access policy

RBAC

#### Answer Area

Enable key vaults for template deployment by using:

A Key Vault access policy

Restrict access to the secrets in Key Vault by using:

A Key Vault access policy

### Explanation:

1) A Key Vault access policy

2) A Key Vault access policy

### Question: 120

CertyIQ

DRAG DROP -

You need to configure access to Azure DevOps agent pools to meet the following requirements:

- ⇒ Use a project agent pool when authoring build or 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 memberships 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 view content.

NOTE: Each correct selection is worth one point.

Select and Place:

## Roles

## Answer Area

Administrator

Organization:

Reader

Project:

Service Account

User

Answer:

## Roles

## Answer Area

Administrator

Organization:

Reader

Reader

Project:

User

### Explanation:

Box 1: Reader -

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

BOX2: User

Members of this role can use the project agent pool when authoring pipelines.

### Question: 121

CertyIQ

You have a branch policy in a project in Azure DevOps. The policy requires that code always builds successfully. You need to ensure that a specific user can always merge changes to the master branch, even if the code fails to compile. The solution must use the principle of least privilege. What should you do?

- A. Add the user to the Build Administrators group.
- B. Add the user to the Project Administrators group.

C. From the Security settings of the repository, modify the access control for the user.

D. From the Security settings of the branch, modify the access control for the user.

**Answer: D**

**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.

Reference:

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

**CertyIQ**

**Question: 122**

You have an Azure Resource Manager template that deploys a multi-tier application.

You need to prevent the user who performs the deployment from viewing the account credentials and connection strings used by the application.

What should you use?

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

**Answer: A**

**Explanation:**

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

Reference:

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

**CertyIQ**

**Question: 123**

SIMULATION -

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 az400-123456789-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 explanation below.

**Explanation:**

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

1. Open the App Service az400-123456789-main, which you want to protect, in the Azure Portal and browse to Settings > Backups. Click Configure and a Backup Configuration blade should appear.
2. Select the storage account.
3. Click + to create a private container. You could name this container after the web app or App Service.
4. Select the container.
5. If you want to schedule backups, then set Scheduled Backup to On and configure a schedule: every five hours
6. Select your retention. Note that 0 means never delete backups.
7. Decide if at least one backup should always be retained.
8. Choose if any connected databases should be included in the web app backup.
9. Click Save to finalize the backup configuration.

The screenshot shows the 'Backup Configuration' blade in the Azure portal. It includes sections for 'Backup Storage' (selecting a storage account), 'Backup Schedule' (configuring scheduled backups every 1 day from January 20, 2018, at 16:31:38 UTC), and 'Backup Database' (selecting a database connection named 'defaultConnection' for backup). The 'Keep at least one backup' option is set to 'Yes'.

Reference:

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

## Question: 124

CertyIQ

SIMULATION -

You need to configure a virtual machine named VM1 to securely access stored secrets in an Azure Key Vault named az400-123456789-kv.

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

### Answer:

See explanation below.

### Explanation:

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

1. Sign in to Azure portal
2. Locate virtual machine VM1.

### 3. Select Identity

### 4. Enable the system-assigned identity for VM1 by setting the Status to On.

A system assigned managed identity enables Azure resources to authenticate to cloud services (e.g. Azure Key Vault) without storing credentials in code. Once enabled, all necessary permissions can be granted via Azure role-based-access-control. The lifecycle of this type of managed identity is tied to the lifecycle of this resource. Additionally, each resource (e.g. Virtual Machine) can only have one system assigned managed identity. [Learn more about Managed identities.](#)

Status: Off → 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-access-nonaad>

## Question: 125

CertyIQ

DRAG DROP -

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.

Select and Place:

### 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

an application registration in contoso.com

a cluster

an RBAC binding

### Explanation:

1. an application registration in contoso.com
2. a cluster
3. an RBAC binding

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli>

The new, improved way: <https://docs.microsoft.com/en-us/azure/aks/managed-aad>

## Question: 126

CertyIQ

### HOTSPOT -

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.

Hot Area:

## Answer Area

Service connection type:

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

Authentication/authorization method for the connection:

|                                         |
|-----------------------------------------|
| Azure Active Directory OAuth 2.0        |
| Grant authorization                     |
| Managed Service Identity Authentication |

**Answer:**

## Answer Area

|                                                             |                                  |
|-------------------------------------------------------------|----------------------------------|
| Service connection type:                                    | <input type="button" value="▼"/> |
| Azure Resource Manager                                      |                                  |
| Generic service                                             |                                  |
| Team Foundation Server / Azure Pipelines service connection |                                  |
| Authentication/authorization method for the connection:     | <input type="button" value="▼"/> |
| Azure Active Directory OAuth 2.0                            |                                  |
| Grant authorization                                         |                                  |
| Managed Service Identity Authentication                     |                                  |

### Explanation:

Box 1: Azure Pipelines service connection

Box 2: Managed Service Identity Authentication

The managed identities for Azure resources feature in Azure Active Directory (Azure AD) provides Azure services with an automatically managed identity in Azure

AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/deploy/azure-key-vault> <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

## Question: 127

CertyIQ

You are deploying a server application that will run on a Server Core installation of Windows Server 2019. You create an Azure key vault and a secret.

You need to use the key vault to secure API secrets for third-party integrations.

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

NOTE: Each correct selection is worth one point.

- A. Configure RBAC for the key vault.
- B. Modify the application to access the key vault.
- C. Configure a Key Vault access policy.
- D. Deploy an Azure Desired State Configuration (DSC) extension.
- E. Deploy a virtual machine that uses a system-assigned managed identity.

**Answer: BCE**

### Explanation:

BE: An app deployed to Azure can take advantage of Managed identities for Azure resources, which allows the app to authenticate with Azure Key Vault using

Azure AD authentication without credentials (Application ID and Password/Client Secret) stored in the app.

C:

1. Select Add Access Policy.
2. Open Secret permissions and provide the app with Get and List permissions.
3. Select Select principal and select the registered app by name. Select the Select button.
4. Select OK.
5. Select Save.
6. Deploy the app.

Reference:

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

CertyIQ

**Question: 128**

HOTSPOT -

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.

Hot Area:

**Answer Area**

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:

**Answer Area**

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:**

Box 1: Microsoft Visual Studio App Center distribution Groups

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

as Staging.

**Box 2: Shared -**

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

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

Reference:

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

**CertyIQ**

**Question: 129**

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

You provision an Azure key vault named Keyvault1.

You need to reference Keyvault1 secrets in a build pipeline of Project1.

What should you do first?

- A. Add a secure file to Project1.
- B. Create an XAML build service.
- C. Create a variable group in Project1.**
- D. Configure the security policy of Contoso.

**Answer: C**

**Explanation:**

Variable group is required to use key vault backed secrets in the pipeline

**CertyIQ**

**Question: 130**

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.

Reference:

**Question: 131**

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:**

Here is my 2 cents, looking at the link by default storage account does not support HTTPS and ARM template comes like below:

"supportsHttpsTrafficOnly": false,

The policy is trying to catch this by using below:

"field": "Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly",

"not Equals": "true"

If you read this carefully it means supports Https Traffic Only - Equals False (which is the default behaviour).. And then action item = DENY. So basically if its not HTTPS or encrypted it has to be denied.. So answer B

Denies non https traffic.

**Question: 132**

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.

Reference:

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

**Question: 133**

**CertyIQ**

DRAG DROP -

You use GitHub Enterprise Server as a source code repository.

You create an Azure DevOps organization named Contoso.

In the Contoso organization, you create a project named Project1.

You need to link GitHub commits, pull requests, and issues to the work items of Project1. The solution must use OAuth-based authentication.

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

Select and Place:

**Actions**

**Answer Area**

From Developer settings in GitHub Enterprise Server, register a new OAuth app.



From Project Settings in Azure DevOps, create a service hook subscription.



From Organization settings in Azure DevOps, connect to Azure Active Directory (Azure AD).

From Project Settings in Azure DevOps, add a GitHub connection.



From Organization settings in Azure DevOps, add an OAuth configuration.



From Developer settings in GitHub Enterprise Server, generate a private key.



**Answer:**

**Actions**

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

**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:**

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:

1. Sign into the web portal for Azure DevOps Services.
2. Add the GitHub Enterprise Oauth configuration to your organization.
3. Open Organization settings>Oauth configurations, and choose Add Oauth configuration.
4. 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>

**Question: 134****CertyIQ**

DRAG DROP -

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.

Select and Place:

**Actions****Answer Area**

Create a service principal in Azure Active Directory (Azure AD).

Add an app registration in Azure Active Directory (Azure AD).

Configure an access policy in the key vault.



Generate a self-signed certificate.

Add an Azure Resource Manager service connection to the pipeline.

Export a certificate from the key vault.

**Answer:****Actions****Answer Area**

Create a service principal in Azure Active Directory (Azure AD).

Create a service principal in Azure Active Directory (Azure AD).

Add an app registration in Azure Active Directory (Azure AD).

Configure an access policy in the key vault.

Configure an access policy in the key vault.

Add an Azure Resource Manager service connection to the pipeline.

Generate a self-signed certificate.



Add an Azure Resource Manager service connection to the pipeline.

Export a certificate from the key vault.

**Explanation:**

Step 1: Create a service principal in Azure Active Directory (Azure AD).

You will need a service principal to deploy an app to an Azure resource from Azure Pipelines.

Step 2: Configure an access policy in the key vault.

You need to secure access to your key vaults by allowing only authorized applications and users. To access the data from the vault, you will need to provide read

(Get) permissions to the service principal that you will be using for authentication in the pipeline.

Select Access policy and then select + Add Access Policy to setup a new policy.

Enable Access to:

- Azure Virtual Machines for deployment ⓘ
- Azure Resource Manager for template deployment ⓘ
- Azure Disk Encryption for volume encryption ⓘ

+ Add Access Policy

Step 3: Add an Azure Resource Manager service connection to the pipeline

You need to authorize the pipeline to deploy to Azure:

1. Select Pipelines | Pipelines,
2. Go to Releases under Pipelines and then select and Edit your pipeline.
3. Under Tasks, notice the release definition for Dev stage has a Azure Key Vault task. This task downloads Secrets from an Azure Key Vault. You will need to point to the subscription and the Azure Key Vault resource.
4. Click Manage, this will redirect to the Service connections page.

The screenshot shows the Azure DevOps Pipeline editor. On the left, there's a list of tasks for a 'Dev' pipeline stage: 'Run on agent', 'Azure Key Vault: mykeyformysql' (selected), 'Azure Deployment:Create Or Update Resource...', and 'Azure App Service Deploy: \${webappName}'. On the right, the 'Azure Key Vault' task configuration pane is open. It shows 'Task version 1.\*' and 'Display name "Azure Key Vault: mykeyformysql"'. Under 'Azure subscription', there is a dropdown menu with a 'Manage' button highlighted by a red box. A note below says '(This setting is required.)'

5. Click on New Service connection -> Azure Resource Manager -> Service Principal (manual). Fill the information from previously created service principal.

Reference:

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

**Question: 135**

CertyIQ

DRAG DROP -

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.

Select and Place:

## 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 -

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>

## Question: 136

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: AD**

**Explanation:**

1. When you use --production flag in NPM install dev Dependencies are not installed (so C is wrong).
2. NPM install command installs the dependencies to the local node modules folder.
3. White Source scan the entire project folder by default. You have to configure it to scan only the node modules since the production dependencies are there.

If there is a policy match on a Reassign action, the request will be automatically reassigned to a designated user or group in the system which is not the default approver."

<https://whitesource.atlassian.net/wiki/spaces/WD/pages/34013519/Managing+Automated+Policies#Applying-Actions-to-a-Library>

<https://whitesource.atlassian.net/wiki/spaces/WD/pages/33751265/Previous+Version+of+WhiteSource+Bolt+for+A-Configuration-for-Azure-DevOps-Server>

<https://docs.npmjs.com/cli/v8/commands/npm-install>

**Question: 137**

**CertyIQ**

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: B**

**Explanation:**

No. CI by itself won't address the issues.

## Question: 138

CertyIQ

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

## Question: 139

CertyIQ

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: A

#### Explanation:

IMO this is the correct answer . I've already explained in the previous answer why Continuous Integration is wrong, and that White source Bolt is not necessarily part of CI. However, White source Bolt \*IS\* an automated security testing solution (which is added to the build pipeline). This answer is more specific, and more correct, than the CI answer.

## Question: 140

CertyIQ

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/>

## Question: 141

CertyIQ

SIMULATION -

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 explanation 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' blade for a SQL database named 'vanazuresqldbserver'. The left sidebar lists various management options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Security, and Advanced Data Security. The 'Advanced Data Security' option is selected and highlighted with a red box. The main content area has two sections: 'VULNERABILITY ASSESSMENT SETTINGS' and 'ADVANCED THREAT PROTECTION SETTINGS'. The 'VULNERABILITY ASSESSMENT SETTINGS' section includes a toggle switch for 'ON' or 'OFF', a 'Subscription' dropdown set to 'SQL DB Content', and a 'Storage account' dropdown. The 'ADVANCED THREAT PROTECTION SETTINGS' section is also highlighted with a red box; it includes a 'Send alerts to' dropdown with 'Email addresses' selected, a checked checkbox for 'Also send email notification to admins and subscription owners', and a dropdown 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>

### Question: 142

CertyIQ

HOTSPOT -

Your company has an Azure subscription.

The company requires that all resource groups 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.

Hot Area:

## Answer Area

```
{
 "policyRule": {
 "if": {
 "allOf": [
 {
 "field": "type",
 "equals": "
 },
 {
 "field": "type",
 "equals": "
 }
]
 },
 "not": {
 "field": "tags['organization']",
 "equals": "Contoso"
 }
 },
 "then": {
 "effect": "
 "details": [
 {
 "field": "tags['organization']",
 "value": "Contoso"
 }
]
 }
}
```

Answer:

#### Answer Area

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

#### Explanation:

"The company requires that all resource groups in the subscription have a tag named organization set to a value of Contoso." - This means also the existing resource groups need to have a tag.

For that reason:

1. Microsoft.Resources/subscriptions/resourceGroups

2. Append

There is a pre-built policy in Azure for this, called: Append a tag and its value to resource groups

CertyIQ

#### Question: 143

You need to configure GitHub to use Azure Active Directory (Azure AD) for authentication. What should you do first?

- A. Create a conditional access policy in Azure AD.
- B. Register GitHub in Azure AD.**
- C. Create an Azure Active Directory B2C (Azure AD B2C) tenant.
- D. Modify the Security settings of the GitHub organization.

#### Answer: B

#### Explanation:

When you connect to a Git repository from your Git client for the first time, the credential manager prompts for credentials. Provide your Microsoft account or Azure AD credentials.

Note: Git Credential Managers simplify authentication with your Azure Repos Git repositories. Credential managers let you use the same credentials that you use for the Azure DevOps Services web portal. Credential managers support multi-factor authentication through Microsoft account or Azure Active Directory (Azure

AD). Besides supporting multi-factor authentication with Azure Repos, credential managers also support two-factor authentication with GitHub repositories.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/set-up-credential-managers>

## Question: 144

CertyIQ

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. Add a deployment gate.
- B. Modify the Deployment queue settings.
- C. Configure a deployment trigger.
- D. Create a pipeline variable.

### Answer: A

#### 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>

## Question: 145

CertyIQ

DRAG DROP -

You have an Azure Kubernetes Service (AKS) implementation that is RBAC-enabled.

You plan to use Azure Container Instances as a hosted development environment to run containers in the AKS implementation.

You need to configure Azure Container Instances as a hosted environment for running the containers in AKS. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

## Actions

Run helm init.

Run az aks install-connector.

Create a YAML file.

Run az role assignment create

Run kubectl apply.

## Answer Area



Answer:

Correct Answer:

### Actions

Run helm init.

Run az aks install-connector.

Create a YAML file.

Run az role assignment create

Run kubectl apply.

### Answer Area

Run kubectl apply.

Run helm init.

Run az aks install-connector.



Explanation:

1. kubectl apply - to create the service principle for Tiller
2. helm init - to deploy Tiller in the kubernetes cluster
3. az aks install-connector - to install the connector

## Question: 146

CertyIQ

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

- A. 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/>

**CertyIQ**

**Question: 147**

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:**

Octopus deploy is solely responsible for automated deployment management. SonarQube is the one that checks for security faults.

**CertyIQ**

**Question: 148**

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>

### Question: 149

CertyIQ

HOTSPOT -

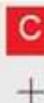
You have a project in Azure DevOps that has three teams as shown in the Teams exhibit. (Click the Teams tab.)

The screenshot shows the 'Teams' section of the Azure DevOps Project Settings. The 'Teams' tab is selected in the left sidebar. The main area displays three teams: Contoso Team (Default), DB Team, and Web Team. The Contoso Team is described as the default project team with 1 member. The DB Team is described as the Parts Unlimited Web Team with 0 members. The Web Team is described as the PUL DB Team with 0 members.

| Name         | Description               | Members |
|--------------|---------------------------|---------|
| Contoso Team | The default project team. | 1       |
| DB Team      | Parts Unlimited Web Team  | 0       |
| Web Team     | PUL DB Team               | 0       |

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.)



## Project Settings

Contoso

General

Overview

Teams

Permissions

Notifications

Service hooks

Dashboards

## Dashboards

Only team admins can set a team's permissions for all dashboards. The permissions set here affect all dashboards for this team.

 Create dashboards ⓘ Edit dashboards ⓘ Delete dashboards ⓘ

All other permissions have the default values set.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

### Statements

**Yes****No**

Web Team can delete Dash1.

Contoso Team can view Dash1.

Project administrators can create new dashboards.

**Answer:**

## Answer Area

### Statements

**Yes****No**

Web Team can delete Dash1.

Contoso Team can view Dash1.

Project administrators can create new dashboards.

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/devops/report/dashboards/charts-dashboard-permissions-access>

### Question: 150

CertyIQ

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

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

What should you use?

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

### 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:

There are several versions of this question in the exam. The question has two possible correct answers:

- ⇒ Black Duck
- ⇒ WhiteSource Bolt

Other incorrect answer options you may see on the exam include the following:

- ⇒ OWASP ZAP
- ⇒ PDM
- ⇒ SourceGear

SourceGear Vault -

Reference:

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

### Question: 151

CertyIQ

DRAG DROP -

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.

Select and Place:

### Answer Area

#### 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

Feed registry information:

Credentials:

### Answer:

### Answer Area

#### 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

Feed registry information: The .npmrc file in the project

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

### Explanation:

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

Feed registry information: The .npmrc file in the project

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

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

On your development machine, you will also have a .npmrc in \$home for Linux or Mac systems or \$env.HOME for win systems. This .npmrc should contain credentials for all of the registries that you need to connect to.

The NPM client will look at your project's .npmrc, discover the registry, and fetch matching credentials from \$home/.npmrc or \$env.HOME/.npmrc.

Reference:

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

### Question: 152

CertyIQ

HOTSPOT -

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.

Hot Area:

## Answer Area

Object to create:

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

Service to use:

|                  |
|------------------|
| WhiteSource Bolt |
| Bamboo           |
| CMake            |
| Chef             |

Answer:

## Answer Area

Object to create:

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

Service to use:

|                  |
|------------------|
| WhiteSource Bolt |
| Bamboo           |
| CMake            |
| Chef             |

### Explanation:

Box 1: A Build task -

Trigger a build -

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

1. Go to Builds section under Pipelines tab, select the build definition WhiteSourceBolt and click on Queue to trigger a build.

2. To view the build in progress status, click on ellipsis and select View build results.

**Box 2: WhiteSource Bolt -**

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

Reference:

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

**Question: 153**

**CertyIQ**

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>

**Question: 154**

**CertyIQ**

DRAG DROP -

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.

Select and Place:

**Commands****Answer Area**

az role assignment create

az aks get-credentials

az aks create

az ad sp create-for-rbac

kubectl create

**Answer:****Correct Answer:****Commands****Answer Area**

az role assignment create

az ad sp create-for-rbac

az aks get-credentials

az aks create

az aks create



az role assignment create

az ad sp create-for-rbac

kubectl create

**Explanation:**

1. az ad sp create-for-rbac - create the service principle
2. az aks create - create the aks with the service principle
3. az role assignment - delegate access to other resources

**Question: 155****CertyIQ**

Your company develops an app for iOS. All users of the app have devices that are members of a private distribution group in Microsoft Visual Studio App Center.

You plan to distribute a new release of the app.

You need to identify which certificate file you require to distribute the new release from App Center.

Which file type should you upload to App Center?

- A. .cer
- B. .pfx
- C. .p12

D. .pvk

#### Answer: C

##### Explanation:

A successful IOS device build will produce an ipa file. In order to install the build on a device, it needs to be signed with a valid provisioning profile and certificate.

To sign the builds produced from a branch, enable code signing in the configuration pane and upload a provisioning profile (.mobileprovision) and a valid certificate (.p12), along with the password for the certificate.

Reference:

<https://docs.microsoft.com/en-us/appcenter/build/xamarin/ios/>

#### Question: 156

CertyIQ

SIMULATION -

You need to prepare a network security group (NSG) named az400-123456789-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.

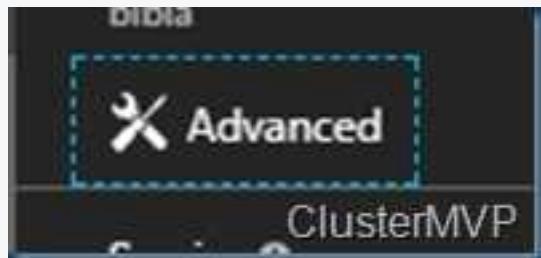
To complete this task, sign in to the Microsoft Azure portal.

##### Answer:

See explanation below.

##### Explanation:

1. Open Microsoft Azure Portal and Log into your Azure account.
2. Select network security group (NSG) named az400-123456789-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.

Reference:

<https://robertsmitt.wordpress.com/2017/09/11/step-by-step-azure-network-security-groups-nsq-security-center-azure-nsq-network/> <https://docs.microsoft.com/en-us/azure/devops/server/architecture/required-ports?view=azure-devops>

#### Question: 157

CertyIQ

DRAG DROP -

You have a project in Azure DevOps named Project1 that contains two Azure DevOps pipelines named Pipeline1 and Pipeline2.

You need to ensure that Pipeline1 can deploy code successfully to an Azure web app named webapp1. The solution

must ensure that Pipeline2 does not have permission to webapp1.

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

Select and Place:

## Actions

## Answer Area

Create a service principal in Azure Active Directory.

In Project1, create a service connection.

In Pipeline1, authorize the service connection.

Create a system-assigned managed identity in Azure Active Directory.

In Project1, configure permissions.

In Pipeline1, create a variable.



### Answer:

#### Correct Answer:

## Actions

## Answer Area

Create a service principal in Azure Active Directory.

In Project1, create a service connection.

In Pipeline1, authorize the service connection.



In Pipeline1, authorize the service connection.

Create a system-assigned managed identity in Azure Active Directory.

In Pipeline1, create a variable.

### Explanation:

1- create a service principle

2- in project 1 create a service connection ( ARM / Manual ) and provide the service principle details created in step 1

3- in pipeline 1, authorize the service connection. this way only pipeline 1 will get access to the webapp and pipeline2 not.

also, project permissions id for users and groups not for pipelines.

### Question: 158

CertyIQ

DRAG DROP -

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.

Select and Place:

## Security Tools

## Answer Area

Penetration testing

Pull request:

Static code analysis

Continuous integration:

Threat modeling

Continuous delivery:

Answer:

Correct Answer:

## Security Tools

## Answer Area

Pull request:

Static code analysis

Continuous integration:

Static code analysis

Continuous delivery:

Penetration testing

Explanation:

Static code

Static code

Penetration

<https://docs.microsoft.com/en-us/azure/devops/migrate/security-validation-cicd-pipeline?view=azure-devops#ide--pull-request>

**Question: 159**

CertyIQ

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. OWASP ZAP
- B. Jenkins
- C. Code Style
- 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.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

- 1. Black Duck
- 2. WhiteSource Bolt

Other incorrect answer options you may see on the exam include the following:

- 1. Microsoft Visual SourceSafe
- 2. PDM
- 3. SourceGear
- 4. SourceGear Vault

Reference:

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

**Question: 160**

CertyIQ

You plan to use a NuGet package in a project in Azure DevOps. The NuGet package is in a feed that requires authentication.

You need to ensure that the project can restore the NuGet package automatically.

What should the project use to automate the authentication?

- A. an Azure Automation account
- B. an Azure Artifacts Credential Provider
- C. an Azure Active Directory (Azure AD) account that has multi-factor authentication (MFA) enabled
- D. an Azure Active Directory (Azure AD) service principal

**Answer: B****Explanation:**

The Azure Artifacts Credential Provider automates the acquisition of credentials needed to restore NuGet

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

Reference:

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

CertyIQ

### Question: 161

You use Azure Pipelines to manage project builds and deployments.

You plan to use Azure Pipelines for Microsoft Teams to notify the legal team when a new build is ready for release. You need to configure the Organization Settings in Azure DevOps to support Azure Pipelines for Microsoft Teams. What should you turn on?

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

Answer: A

**Explanation:**

The Azure Pipelines app uses the OAuth authentication protocol, and requires Third-party application access via OAuth for the organization to be enabled. To enable this setting, navigate to Organization Settings > Security > Policies, and set the 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>

CertyIQ

### Question: 162

You have an existing project in Azure DevOps.

You plan to integrate GitHub as the repository for the project.

You need to ensure that Azure Pipelines runs under the Azure Pipelines identity.

Which authentication mechanism should you use?

- A. personal access token (PAT)
- B. GitHub App
- C. Azure Active Directory (Azure AD)
- D. OAuth

Answer: B

**Explanation:**

GitHub App uses the Azure Pipelines identity.

Incorrect Answers:

A: Personal access token and OAuth use your personal GitHub identity.

Reference:

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

## Question: 163

DRAG DROP -

You have an Azure subscription that uses Azure Monitor and contains a Log Analytics workspace.

You have an encryption key.

You need to configure Azure Monitor to use the key to encrypt log data.

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 correct orders you select.

Select and Place:

### Actions

### Answer Area

Configure the key vault properties for the cluster



Link the Log Analytics workspace to the cluster

Grant the system-assigned managed identity Key permissions for the key vault

Grant the system-assigned managed identity Certificate permissions for the key vault

Create an Azure Monitor Logs dedicated cluster that has a system-assigned managed identity

Create an Azure key vault and store the key

### Answer:

### Actions

### Answer Area

Grant the system-assigned managed identity Certificate permissions for the key vault



Create an Azure key vault and store the key

Create an Azure Monitor Logs dedicated cluster that has a system-assigned managed identity

Grant the system-assigned managed identity Key permissions for the key vault

Configure the key vault properties for the cluster

Link the Log Analytics workspace to the cluster

### Explanation:

Customer-Managed key provisioning steps:

Step 1: Create an Azure Key vault and store the key.

Creating Azure Key Vault and storing key. Create or use an existing Azure Key Vault in the region that the cluster is planned, and generate or import a key to be used for logs encryption.

Step 2: Create an Azure Monitor Logs dedicate cluster that has a system-assigned managed identity

Clusters uses managed identity for data encryption with your Key Vault. Configure identity type property to SystemAssigned when creating your cluster to allow access to your Key Vault for "wrap" and "unwrap" operations.

Step 3: Grant the system-assigned managed Identity Key permissions for the key vault.

Grant Key Vault permissions.

Create Access Policy in Key Vault to grants permissions to your cluster. These permissions are used by the underlay cluster storage. Open your Key Vault in

Azure portal and click Access Policies then + Add Access Policy to create a policy with these settings:

"Key permissions"select Get, Wrap Key and Unwrap Key.

**Add access policy**

Add access policy

Configure from template (optional)

Key permissions

3 selected

- Select all
- Key Management Operations**
- Get
  - List
  - Update
  - Create
  - Import
  - Delete
  - Recover
  - Backup
  - Restore

Secret permissions

0 selected

Certificate permissions

0 selected

Select principal

Cluster resource principle-id

Authorized application ⓘ

None selected

**Add**

- Decrypt
- Encrypt
- Unwrap Key
- Wrap Key
- Verify
- Sign
- Cryptographic Operations**
- Purge
- Privileged Key Operations**

**1. Creating cluster**

2. Granting permissions to your Key Vault

3. Updating cluster with key identifier details

4. Linking workspaces

Step 4: Configure the key vault properties for the cluster.

Update cluster with key identifier details.

Step 5: Link the Log Analytics workspace to the cluster

Link workspace to cluster.

This step should be performed only after the cluster provisioning. If you link workspaces and ingest data prior to the provisioning, ingested data will be dropped and won't be recoverable.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/customer-managed-keys>

**Question: 164****CertyIQ**

DRAG DROP -

You have an Azure Key Vault that contains an encryption key named key1.

You plan to create a Log Analytics workspace that will store logging data.

You need to encrypt the workspace by using key1.

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.

Select and Place:

**Actions**

- Link the workspace.
- Register the Azure subscription to allow cluster creation.
- Grant permissions to the key vault.
- Create a Log Analytics cluster.
- Enable soft delete for the key vault.

**Answer Area****Answer:****Correct Answer:****Actions**

- Register the Azure subscription to allow cluster creation.

**Answer Area**

- Register the Azure subscription to allow cluster creation.
- Create a Log Analytics cluster.
- Grant permissions to the key vault.
- Link the workspace.

**Explanation:**

1. Register the Azure subscription to allow cluster creation.
2. Create a Log Analytics cluster.
3. Grant permissions to the key vault.
4. Link the workspace.

**Question: 165****CertyIQ**

You use release pipelines in Azure Pipelines to deploy an app. Secrets required by the pipeline are stored as pipeline variables. Logging of commands is enabled for the Azure Pipelines agent.

You need to prevent the values of the secrets from being logged.

What should you do?

- A. Store the secrets in the environment variables instead of the pipeline variables.
- B. Pass the secrets on the command line instead of in the pipeline variables.
- C. Apply a prefix of secret to the name of the variables.
- D. Echo the values of the secrets to the command line.

**Answer: A****Explanation:**

Don't set secret variables in your YAML file. Operating systems often log commands for the processes that

they run, and you wouldn't want the log to include a secret that you passed in as an input. Use the script's environment or map the variable within the variables block to pass secrets to your pipeline.

#### Incorrect Answers:

B: Never pass secrets on the command line.

C: Adding a prefix does not make the variable a secret. The `issecret` property makes it secret but does not prevent logging of the secret.

D: Never echo secrets as output.

#### Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/process/variables?view=azure-devops&tabs=yaml%2Cbatch>

<https://docs.microsoft.com/en-us/azure/devops/pipelines/scripts/logging-commands?view=azure-devops&tabs=bash>

## Question: 166

CertyIQ

#### DRAG DROP -

You need to deploy a new project in Azure DevOps that has the following requirements:

\* The lead developer must be able to create repositories, manage permissions, manage policies, and contribute to the repository.

\* Developers must be able to contribute to the repository and create branches, but NOT bypass policies when pushing builds.

\* Project managers must only be able to view the repository.

\* The principle of least privilege must be used.

You create a new Azure DevOps project team for each role.

To which Azure DevOps groups should you add each team? To answer, drag the appropriate groups to the correct teams. 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.

Select and Place:

Azure DevOps groups

- Build Administrators
- Contributors
- Project Administrators
- Project Collection Administrators
- Project Collection Valid Users
- Readers

#### Answer Area

Project manager:

Azure DevOps group

Lead developer:

Azure DevOps group

Developer:

Azure DevOps group

## Answer:

Azure DevOps groups

- Build Administrators
- Contributors
- Project Administrators
- Project Collection Administrators
- Project Collection Valid Users
- Readers

#### Answer Area

Project manager:

Readers

Lead developer:

Project Administrators

Developer:

Contributors

## Explanation:

Box 1: Readers -

Project managers must only be able to view the repository.

Only read permission necessary.

Box 2: Project Administrators -

The lead developer must be able to create repositories, manage permissions, manage policies, and contribute to the repository.

Add to the Project Collection Administrators security group users tasked with managing organization or collection resources.

**Box 3: Contributors -**

Developers must be able to contribute to the repository and create branches, but NOT bypass policies when pushing builds.

Add to the Contributors security group full-time workers who contribute to the code base or manage projects.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/organizations/security/look-up-project-collection-administrators>

### Question: 167

CertyIQ

DRAG DROP -

You have an Azure subscription that contains a project in Azure DevOps named Project1. You have three Azure Active Directory (Azure AD) users that require access to Project1 as shown in the following table.

| Name  | Title            | Requirement                                 |
|-------|------------------|---------------------------------------------|
| User1 | Project Manager  | View repositories.                          |
| User2 | Development Lead | Create repositories and manage permissions. |
| User3 | Developer        | Create branches and tags.                   |

You need to ensure that the users have the appropriate permissions. The solution must use the principle of least privilege.

To which permission group in Azure DevOps should you add each user? To answer, drag the appropriate permission groups to the correct users. Each permission 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.

#### Permission Groups

Build Administrators

Contributors

Project Administrators

Readers

#### Answer Area

User1:

User2:

User3:

Answer:

## Answer Area

User1: Readers

User2: Project Administrators

User3: Contributors

### Question: 168

CertyIQ

You have an Azure subscription linked to an Azure Active Directory Premium Plan 1 tenant.

A security review indicates that too many users have privileged access to resources.

You need to deploy a privileged access management solution that meets the following requirements:

- Enforces time limits on the use of privileged access
- Requires approval to activate privileged access
- Minimizes costs

What should you do first?

- A. Configure notifications when privileged roles are activated.
- B. Configure alerts for the activation of privileged roles.
- C. Enforce Azure Multi-Factor Authentication (MFA) for role activation.
- D. Upgrade the license of the Azure Active Directory (Azure AD) tenant.

Answer: D

### Question: 169

CertyIQ

You plan to create a GitHub workflow that will use GitHub Actions. The actions will require a 256-KB secret.

You need to recommend a solution to store and encrypt the secret. The secret value must be accessible only to the workflow. The solution must minimize administrative effort

What should you recommend?

- A. Store the secret in the organization-level GitHub secrets.
- B. Store the secret in the repository-level GitHub secrets.
- C. Encrypt the secret value and store the value in the repository. Store the decryption key in the repository-level GitHub secrets.
- D. Encrypt the secret value and store the value in the repository. Store the decryption key in the organization-level GitHub secrets.

Answer: C

Explanation:

To use secrets that are larger than 48 KB, you can use a workaround to store encrypted secrets in your repository and save the decryption passphrase as a secret on GitHub." Because it requires less administrative

privilege it's at repository level

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

CertyIQ

### Question: 170

You have a GitHub Enterprise account.

You need to enable push protection for secret scanning of the account repositories.

What should you do first?

- A. Purchase a GitHub Advanced Security license.
- B. Purchase Premium Plus support.
- C. Enforce multi-factor authentication (MFA).
- D. Create an access policy for secrets.

### Answer: A

#### Explanation:

Secret scanning alerts for partners run automatically on all public repositories. If you have a license for GitHub Advanced Security, you can enable and configure secret scanning alerts for users for any repository owned by an organization.

[https://docs.github.com/en/\[email protected\]/code-security/secret-scanning/protecting-pushes-with-secret-scanning](https://docs.github.com/en/[email protected]/code-security/secret-scanning/protecting-pushes-with-secret-scanning)

CertyIQ

### Question: 171

DRAG DROP -

Your company has a project in Azure DevOps named Project1.

All the developers at the company have Windows 10 devices.

You need to create a Git repository for Project1. The solution must meet the following requirements:

- Support large binary files.
- Store binary files outside of the repository.
- Use a standard Git workflow to maintain the metadata of the binary files by using commits to the repository.

Which three actions should you perform in sequence on each developer's device? 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

Configure SSH key-based authentication.

Configure personal access token (PAT)-based authentication.

Perform a custom installation of Git for Windows that includes Git Virtual File System (GVFS).

Configure Git Large File Storage (LFS) file tracking.

Perform a custom installation of Git for Windows that includes Git Large File Storage (LFS).



## Answer:

### Actions

### Answer Area

Configure SSH key-based authentication.

Configure personal access token (PAT)-based authentication.

Configure personal access token (PAT)-based authentication.

Perform a custom installation of Git for Windows that includes Git Large File Storage (LFS).

Perform a custom installation of Git for Windows that includes Git Virtual File System (GVFS).

Configure Git Large File Storage (LFS) file tracking.

Configure Git Large File Storage (LFS) file tracking.



## Explanation:

Configure PAT

Perform installation of Git LFS

Track GIT LFS

<https://docs.github.com/en/repositories/working-with-files/managing-large-files/about-git-large-file-storage>

## Question: 172

CertyIQ

You have an Azure subscription that contains four Azure virtual machines.

You need to configure the virtual machines to use a single identity. The solution must meet the following requirements:

- Ensure that the credentials for the identity are managed automatically.
- Support granting privileges to the identity.

Which type of identity should you use?

- A.a system-assigned managed identity
- B.a user-assigned managed identity**
- C.a service principal
- D.a user account

**Answer: B**

**Explanation:**

B is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview#managed-identity-types>. User-assigned. You may also create a managed identity as a standalone Azure resource. You can create a user-assigned managed identity and assign it to one or more Azure Resources. When you enable a user-assigned managed identity:-- A service principal of a special type is created in Azure AD for the identity. The service principal is managed separately from the resources that use it.-- User-assigned identities can be used by multiple resources.-- You authorize the managed identity to have access to one or more services

B. a user-assigned managed identity.A user-assigned managed identity is an identity that you create as a standalone Azure resource and can be assigned to multiple Azure resources. It allows you to use the same identity across multiple virtual machines, providing consistent and centralized management.

**Question: 173**

**CertyIQ**

HOTSPOT

-

You have an Azure subscription that contains an Azure key vault named Vault1, an Azure pipeline named Pipeline1, and an Azure SQL database named DB1.

Pipeline1 is used to deploy an app that will authenticate to DB1 by using a password.

You need to store the password in Vault1. The solution must ensure that the password can be accessed by Pipeline1.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Store the password as a:

|             |   |
|-------------|---|
| Certificate | ▼ |
| Key         |   |
| Secret      |   |

Grant Pipeline1 access to Vault1 by modifying the:

|                               |   |
|-------------------------------|---|
| Access control (IAM) settings | ▼ |
| Access policies               |   |
| Security settings             |   |

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

Store the password as a:

Grant Pipeline1 access to Vault1 by modifying the:

**Explanation:**

1. Secret
2. Access policy

<https://learn.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal>

A Key Vault access policy determines whether a given security principal, namely a user, application or user group, can perform different operations on Key Vault secrets, keys, and certificates. You can assign access policies using the Azure portal, the Azure CLI, or Azure PowerShell.

**Question: 174****CertyIQ**

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

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

What should you do first?

- A. Recreate the secret at the organization level.
- B. Recreate the secret at the repository level.**
- C. Enable required reviewers.

**Answer: B****Explanation:**

B is the answer.

<https://docs.github.com/en/actions/security-guides/encrypted-secrets#creating-encrypted-secrets-for-a-repository>

**Question: 175****CertyIQ**

DRAG DROP

You have a GitHub organization that contains three users named User1, User2, and User3. You have a project that contains a repository named repo1.

You need to configure permissions for repo1. The solution must meet the following requirements:

- Ensure that User1 can actively push to repo1.

- Ensure that User2 can manage issues and pull requests for repo1.
- Ensure that User3 can manage repo1.
- Prevent User3 from accessing sensitive data in repo1.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role 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.

### Roles

- Admin
- Maintain
- Read
- Triage
- Write

### Answer Area

- User1:
- User2:
- User3:

Answer:

### Answer Area

User1: Write

User2: Triage

User3: Maintain

### Question: 176

CertyIQ

You are designing the development process for your company.

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

What should you include in the recommendation?

- A. Microsoft Visual Studio test plans
- B. Gradle wrapper scripts
- C. SonarCloud analysis**
- D. the JavaScript task runner

Answer: C

Explanation:

SonarCloud is a cloud service offered by SonarSource and based on SonarQube. SonarQube is a widely

adopted open source platform to inspect continuously the quality of source code and detect bugs, vulnerabilities and code smells in more than 20 different languages.

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

Incorrect Answers:

A: Test plans are used to group together test suites and individual test cases. This includes static test suites, requirement-based suites, and query-based suites.

Reference:

<https://docs.travis-ci.com/user/sonarcloud/>

<https://sonarcloud.io/documentation/integrations/vsts/>

## Question: 177

CertyIQ

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: A

Explanation:

You recommend reducing the code coupling and the dependency cycles" is a part of reducing code complexity.

## Question: 178

CertyIQ

Your company uses Azure DevOps for the build pipelines and deployment pipelines of Java-based projects.

You need to recommend a strategy for managing technical debt.

Which two actions should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Configure post-deployment approvals in the deployment pipeline.

B. **Configure pre-deployment approvals in the deployment pipeline.**

C. Integrate Azure DevOps and SonarQube.

D. Integrate Azure DevOps and Azure DevTest Labs.

Answer: BC

Explanation:

B: With SonarQube pre-approval, you can set quality gate.

C: You can manage technical debt with SonarQube and Azure DevOps.

Note: Technical debt is the set of problems in a development effort that make forward progress on customer value inefficient. Technical debt saps productivity by making code hard to understand, fragile, time-consuming to change, difficult to validate, and creates unplanned work that blocks progress. Unless they are managed, technical debt can accumulate and hurt the overall quality of the software and the productivity of the development team in the long term

SonarQube an open source platform for continuous inspection of code quality to perform automatic reviews with static analysis of code to:

- ⇒ Detect Bugs
- ⇒ Code Smells
- ⇒ Security Vulnerabilities
- ⇒ Centralize Quality
- ⇒ What's covered in this lab

Reference:

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

## Question: 179

CertyIQ

Your company is building a new solution in Java.

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

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

Which task types should you add to the build pipeline?

- A. Gradle
- B. CocoaPods
- C. Grunt
- D. Gulp

### Answer: A

#### 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.

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.

Incorrect Answers:

B: CocoaPods is the dependency manager for Swift and Objective-C Cocoa projects.

Note: There are several versions of this question in the exam. The question can have three correct answers:

- ⇒ MSBuild
- ⇒ Maven
- ⇒ Gradle

The question can also have different incorrect options, including:

- ⇒ Chef
- ⇒ Octopus
- ⇒ xCODE

Reference:

<https://docs3.sonarqube.org/latest/analysis/scan/sonarscanner-for-azure-devops/>  
<https://docs.microsoft.com/en-us/azure/devops/java/sonarqube?view=azure-devops>

### Question: 180

CertyIQ

HOTSPOT -

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.

Hot Area:

## Answer Area

Convert the .docx files to:

|                                 |
|---------------------------------|
| LaTeX Typesetting (.tex)        |
| Markdown (.md)                  |
| Portable Document Format (.pdf) |

Convert the flow charts to:

|                                  |
|----------------------------------|
| Mermaid diagrams                 |
| Portable Network Graphics (.png) |
| Tagged Image File Format (.tiff) |

Answer:

## Answer Area

Convert the .docx files to:

- LaTex Typesetting (.tex)
- Markdown (.md)**
- Portable Document Format (.pdf)

Convert the flow charts to:

- Mermaid diagrams**
- Portable Network Graphics (.png)
- Tagged Image File Format (.tiff)

### Explanation:

Box 1: Markdown (.md)

Github understands several text formats, including .txt and .md. .md stands for a file written in Markdown.

Box 2: Mermaid diagrams -

Mermaid lets you create diagrams and visualizations using text and code.

It is a Javascript based diagramming and charting tool that renders Markdown-inspired text definitions to create and modify diagrams dynamically.

Reference:

<https://ourcodingclub.github.io/tutorials/git/>

<https://mermaid-js.github.io/mermaid/#/>

CertyIQ

### Question: 181

Your company is building a new solution in Java.

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

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

Which task types should you add to the build pipeline?

- A. Grunt
- B. Octopus
- C. Maven**
- D. Gulp

### Answer: C

### Explanation:

SonarQube is a set of static analyzers that can be used to identify areas of improvement in your code. It allows you to analyze the technical debt in your project and keep track of it in the future. With Maven and Gradle build tasks, you can run SonarQube analysis with minimal setup in a new or existing Azure DevOps Services build task.

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.

Note: There are several versions of this question in the exam. The question can have three correct answers:

- ⇒ MSBuild
- ⇒ Maven
- ⇒ Gradle

The question can also have different incorrect options, including:

- ⇒ Chef
- ⇒ xCODE
- ⇒ CocoaPods

Reference:

<https://docs3.sonarqube.org/latest/analysis/scan/sonarscanner-for-azure-devops/> <https://docs.microsoft.com/en-us/azure/devops/java/sonarqube?view=azure-devops>

## Question: 182

CertyIQ

DRAG DROP -

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

You need to configure SonarQube to perform a code quality validation of the C# code as part of the build pipelines. Which four tasks should you perform in sequence? To answer, move the appropriate tasks from the list of tasks to the answer area and arrange them in the correct order.

Select and Place:

### Actions Commands Cmdlets Statements

Run Code Analysis

Visual Studio Test

Publish Build Artifacts

Visual Studio Build

Prepare Analysis Configuration

### Answer Area

## Answer:

### Actions Commands Cmdlets Statements

Run Code Analysis

Visual Studio Test

Publish Build Artifacts

Visual Studio Build

Prepare Analysis Configuration

### Answer Area

Prepare Analysis Configuration

Visual Studio Build

Visual Studio Test

Run Code Analysis

## Explanation:

Step 1: Prepare Analysis Configuration

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

This task is mandatory.

In case of .NET solutions or Java projects, it helps to integrate seamlessly with MSBuild, Maven and Gradle tasks.

**Step 2: Visual Studio Build -**

Reorder the tasks to respect the following order:

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

**Step 3: Visual Studio Test -**

Reorder the tasks to respect the following order:

Run Code Analysis task after the Visual Studio Test task.

**Step 4: Run Code Analysis -**

Run Code Analysis task, to actually execute the analysis of the source code.

This task is not required for Maven or Gradle projects, because scanner will be run as part of the Maven/Gradle build.

Note:



Reference:

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

### Question: 183

CertyIQ

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 an open source platform for continuous inspection of code quality to perform automatic reviews with static analysis of code to:

- ⇒ Detect Bugs
- ⇒ Code Smells
- ⇒ Security Vulnerabilities
- ⇒ Centralize Quality
- ⇒ What's covered in this lab

Reference:

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

CertyIQ

### Question: 184

DRAG DROP -

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.

Select and Place:

#### 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:

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

Reference:

<https://docs.microsoft.com/en-us/azure/devops/boards/queries/link-work-items-support-traceability?view=azure-devops&tabs=new-web-for-m> <https://docs.microsoft.com/en-us/visualstudio/releasenotes/tfs2017-relnotes>

### Question: 185

CertyIQ

DRAG DROP -

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.

Select and Place:

#### Actions

#### Answer Area

Create a new Azure Artifacts feed.

Configure a self-hosted agent.

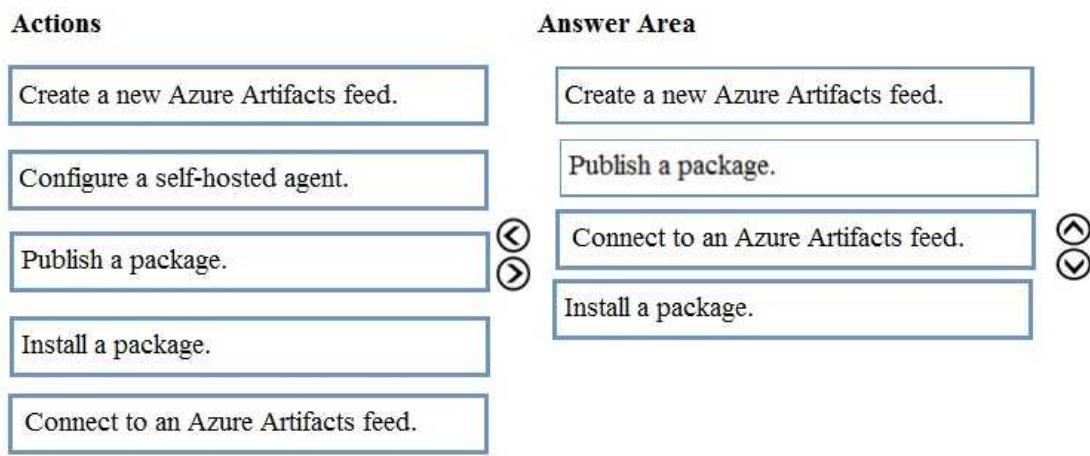
Publish a package.

Install a package.

Connect to an Azure Artifacts feed.



Answer:



### Explanation:

1. Create
2. Publish
3. Connect
4. Install

### Question: 186

CertyIQ

During a code review, you discover many quality issues. Many modules contain unused variables and empty catch blocks.

You need to recommend a solution to improve the quality of the code.

What should you recommend?

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

### Answer: B

#### Explanation:

PMD is a source code analyzer. It finds common programming flaws like unused variables, empty catch blocks, unnecessary object creation, and so forth.

There is an Apache Maven PMD Plugin which allows you to automatically run the PMD code analysis tool on your project's source code and generate a site report with its results.

Incorrect Answers:

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

Reference:

<https://pmd.github.io>

/

**Question: 187**

CertyIQ

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: BAE****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.

Reference:

<https://medium.com/medialesson/get-started-with-private-nuget-feeds-in-azure-devops-8c7b5f022a68>

**Question: 188**

CertyIQ

You use GitHub for source control.

A file that contains sensitive data is committed accidentally to the Git repository of a project.

You need to delete the file and its history from the repository.

Which two tools can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. the git filter-branch command
- B. BFG Repo-Cleaner
- C. the git rebase command
- D. GitHub Desktop

**Answer: AB**

**Explanation:**

To entirely remove unwanted files from a repository's history you can use either the git filter-branch command or the BFG Repo-Cleaner open source tool.

Reference:

<https://docs.github.com/en/github/authenticating-to-github/keeping-your-account-and-data-secure/removing-sensitive-data-from-a-repository>

**Question: 189**

CertyIQ

Your company uses GitHub for source control. The company has a team that performs code reviews.

You need to automate the assignment of the code reviews. The solution must meet the following requirements:

- ⇒ Prioritize the assignment of code reviews to team members who have the fewest outstanding assignments.
- ⇒ Ensure that each team member performs an equal number of code reviews in any 30-day period.
- ⇒ Prevent the assignment of code reviews to the team leader.

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

NOTE: Each correct selection is worth one point.

- A. Clear Never assign certain team members.
- B. Select If assigning team members, don't notify the entire team.
- C. Select Never assign certain team members.**
- D. Set Routing algorithm to Round robin.
- E. Set Routing algorithm to Load balance.**

**Answer: CE**

**Explanation:**

Optionally, to always skip certain members of the team, select Never assign certain team members. Then, select one or more team members you'd like to always skip" ---> C (prevent assignment to Leader)

"The load balance algorithm chooses reviewers based on each member's total number of recent review requests and considers the number of outstanding reviews for each member. The load balance algorithm tries to ensure that each team member reviews an equal number of pull requests in any 30 day period." ---> E (Ensure that each team member performs an equal number of code reviews in any 30-day period)

<https://docs.github.com/en/organizations/organizing-members-into-teams/managing-code-review-settings-for-your-team>

**Question: 190**

CertyIQ

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.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/import-git-repository?view=azure-devops>

**CertyIQ****Question: 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.

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.

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/>

**CertyIQ****Question: 192**

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.

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/>

CertyIQ

#### Question: 193

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

#### Explanation:

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/>

CertyIQ

#### Question: 194

During a code review, you discover quality issues in a Java application.

You need to recommend a solution to detect quality issues including unused variables and empty catch blocks.

What should you recommend?

A. In a Maven build task, select Run PMD.

B. In an Xcode build task, select Use xcpretty from Advanced.

C. In a Gulp build task, specify a custom condition expression.

D. In a Grunt build task, select Enabled from Control Options.

#### Answer: A

##### Explanation:

PMD is a source code analyzer. It finds common programming flaws like unused variables, empty catch blocks, unnecessary object creation, and so forth.

There is an Apache Maven PMD Plugin which allows you to automatically run the PMD code analysis tool on your project's source code and generate a site report with its results.

Incorrect Answers:

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

Reference:

<https://pmd.github.io/>

CertyIQ

#### Question: 195

You use Azure Artifacts to host NuGet packages that you create.

You need to make one of the packages available to anonymous users outside your organization. The solution must minimize the number of publication points.

What should you do?

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

#### Answer: D

##### Explanation:

Publish the package to a public NuGet repository. This is because to use the public feed feature in Azure DevOps, the project itself must be public: "Public feeds are project-scoped feeds that live inside a public project. You cannot convert an existing organization-scoped feed into a project-scoped feed or a public feed."

<https://docs.microsoft.com/en-us/azure/devops/artifacts/tutorials/share-packages-publicly?view=azure-devops>

CertyIQ

#### Question: 196

You use GitHub for source control and project-related discussions.

You receive a notification when an entry is made to any team discussion.

You need to ensure that you receive email notifications only for discussions in which you commented or in which you are mentioned.

Which two Notifications settings should you clear? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Automatically watch teams
- B. Participating**
- C. Automatically watch repositories
- D. Watching**

**Answer: BD**

**Explanation:**

"If you don't want notifications to be sent to your email, unselect email for participating and watching notifications.

If you want to receive notifications by email when you've participated in a conversation, then you can select email under "Participating".

If you do not enable watching or participating notifications for web and mobile, then your notifications inbox will not have any updates." b and d

**Question: 197**

**CertyIQ**

You have an Azure Automation account that contains a runbook. The runbook is used to configure the application infrastructure of an Azure subscription.

You have a project in Azure DevOps named Project1. Project1 contains a repository that stores code for the runbook.

You need to ensure that every committed change to the code will update automatically and publish the runbook to Azure Automation.

What should you configure?

- A. the Service hooks settings for Project1
- B. the Connections settings for the Automation account
- C. the Source control settings for the Automation account**
- D. the Service connections settings for Project1

**Answer: C**

**Explanation:**

Source control allows you to ensure that all of your Azure Automation runbooks are up-to-date with your scripts in an external source control. Click 'Add' to create a new source control configuration which will import all of the runbooks within a given folder in your external source control to your Automation account.

**Question: 198**

**CertyIQ**

You use Git for source control.

You enable GitHub code scanning.

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

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

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

NOTE: Each correct selection is worth one point.

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

- B. Add the name of the non-default branch to the on:push specification in the code scanning workflow.
- C. Delete the pull request, and then raise the request again from the default branch.
- D. Update the code in the pull request.
- E. Add a new workflow for code scanning.

**Answer: BD**

**Explanation:**

There are other situations where there may be no analysis for the latest commit to the base branch for a pull request. These include:

The pull request has been raised against a branch other than the default branch, and this branch hasn't been analyzed.

The solution in this situation is to add the name of the base branch to the onpush [THIS IS ANSWER B] and on:pull request specification in the code scanning workflow on that branch and then make a change that updates the open pull request that you want to scan [THIS IS ANSWER D].

[https://docs.github.com/en/\[email protected\]/code-security/code-scanning/automatically-scanning-your-code-for-vulnerabilities-and-errors/configuring-code-scanning-for-a-repository](https://docs.github.com/en/[email protected]/code-security/code-scanning/automatically-scanning-your-code-for-vulnerabilities-and-errors/configuring-code-scanning-for-a-repository)

## Question: 199

CertyIQ

DRAG DROP

You have a GitHub repository named repo1 that stores the code of an app named App1.

You need deploy a workflow for repo1 by using GitHub Actions. The solution must meet the following requirements:

- Scan on pushes to the main branch.
- Scan on pull requests to the main branch.
- Scan on pull requests to any branch that has a prefix of releases/.
- Scan all the files in the subdirectories of the src directory.
- Exclude scanning of markdown files.

How should you complete the code? To answer, drag the appropriate values to the correct targets. 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

- '\*\*/\*.md'

- '\*\*.md'

- 'release\*\*'

- 'releases/\*\*'

- 'src/\*\*'

- 'src/\*\*'

## Answer Area

\*\*\*

on:

push:

branches: [main]

pull\_request:

branches:

- main

paths:

paths-ignore:

\*\*\*

Answer:

## Answer Area

```

on:

push:

 branches: [main]

pull_request:

 branches:

- main

 - 'releases/**'

paths:

 - 'src/**'

paths-ignore:

 - '**/*.md'

```

### Question: 200

CertyIQ

You have a GitHub repository that contains multiple versions of an Azure Pipelines template.

You plan to deploy multiple pipelines that will use a template stored in the repository.

You need to ensure that you use a fixed version of the template.

What should you use to reference which version of the template repository to use?

- A. the serial
- B. the SHA-based hashes
- C. the runner
- D. the branch

### Answer: D

#### Explanation:

If you want to use a particular, fixed version of the template, be sure to pin to a ref. The refs are either branches (refs/heads/<name>) or tags (refs/tags/<name>). If you want to pin a specific commit, first create a tag pointing to that commit, then pin to that tag.

<https://learn.microsoft.com/en-us/azure/devops/pipelines/process/templates?view=azure-devops#use-other-repositories>

### Question: 201

CertyIQ

DRAG DROP

You have the repositories shown in the following table.

| Type        | URL                                                                                                                             |
|-------------|---------------------------------------------------------------------------------------------------------------------------------|
| Azure Repos | <a href="https://dev.azure.com/contoso/project1/_git/project1.git">https://dev.azure.com/contoso/project1/_git/project1.git</a> |
| GitHub      | <a href="https://github.com/contoso/project.git">https://github.com/contoso/project.git</a>                                     |

You need to migrate the contents of the GitHub repository to the Azure Repos repository. The solution must ensure that the Azure Repos repository only contains branches and history from the GitHub repository.

Which three commands should you 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

```
git clone --bare
https://dev.azure.com/contoso/project1/_git/proj
```

```
cd project1
```

```
git clone --bare
https://github.com/contoso/project1.git
```

```
git push --mirror
https://dev.azure.com/contoso/project1/_git/proj
```

```
cd project1.git
```

```
git push --mirror
https://github.com/contoso/project1.git
```

#### Answer Area



Answer:

## Answer Area

```
git clone --bare
https://github.com/contoso
/project1.git
```

```
cd project1.git
```

```
git push --mirror
https://dev.azure.com/contoso
/project1/_git/proj
```

### Question: 202

CertyIQ

DRAG DROP

You have a GitHub repository that contains the code for an app named App1.

App1 depends on a library of functions from a repository at <https://github.com/contoso/afeed>.

You need to keep a clone of the afeed repository as a subdirectory of the App1 repository.

How should you complete the Git command? To answer, drag the appropriate values to the correct targets. 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

git   <https://github.com/contoso/afeed>

Answer:

**Values****Answer Area** add branch clone

git submodule add https://github.com/contoso/afeed

 pull submodule**Explanation:**

git submodule add

<https://git-scm.com/book/en/v2/Git-Tools-Submodules>

**Question: 203****CertyIQ****HOTSPOT**

-

You use Git for source control.

You need to optimize the performance of a repository. The solution must meet the following requirements:

- Permanently remove all items referenced only in the reflog.
- Remove history that is NOT in any current branch.

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

NOTE: Each correct selection is worth one point.

## Answer Area

git expire --expire-unreachable=now --all

git --prune=

The first dropdown menu contains: gc, reflog, reset, stash.

The second dropdown menu contains: all, now, reset, true.

Answer:

## Answer Area

git expire --expire-unreachable=now --all

git --prune=

The first dropdown menu contains: gc, reflog, reset, stash. The item 'reflog' is highlighted with a red box.

The second dropdown menu contains: all, now, reset, true. The item 'now' is highlighted with a red box.

### Question: 204

CertyIQ

DRAG DROP

You have an Azure Repos Git repository named repo1.

You need to ensure that you can authenticate to repo1 by using SSH.

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

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

## Actions

Sign in to Azure DevOps.

Add the SSH public key.

Clone repo1.

Save the SSH key to the root of repo1.

Add the SSH private key.

Create SSH keys by using ssh-keygen

## Answer Area



### Answer:

#### Answer Area

Create SSH keys by using ssh-keygen

Sign in to Azure DevOps.

Add the SSH public key.

Clone repo1.

### Explanation:

Create ssh keys using ssh-keygen

Sign into azure devOps

Add the SSH public key

Clone repo1

You use Git for source control.

You delete a file, commit the changes, and continue to work.

You need to recover the deleted file.

Which three commands should you 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

git commit -m 'undeleted the file'

git log

git checkout [hash]~1 --path/to/file

git tag

git restore path/to/file

git stash



### Answer:

#### Commands

#### Answer Area

git commit -m 'undeleted the file'

git log

git checkout [hash]~1 --path/to/file

git tag

git restore path/to/file

git stash

git stash

git log

git checkout [hash]~1 --path/to/file



### Explanation:

git stash

git log

git checkout [hash]~1

## HOTSPOT

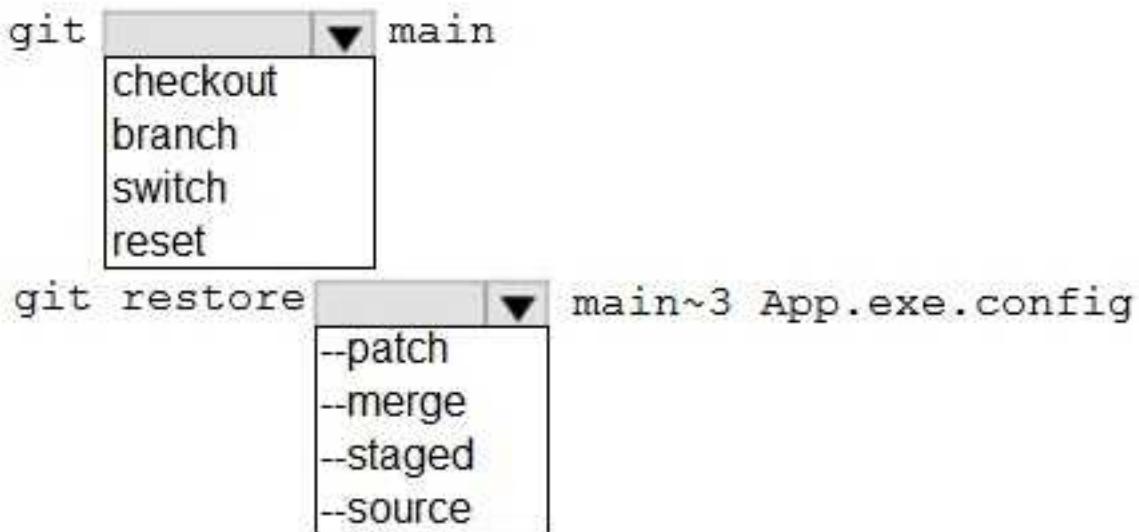
You use Git for source control. You have an app named App1.

In the main branch, you need to restore the third most recent revision of a file named App.exe.config.

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

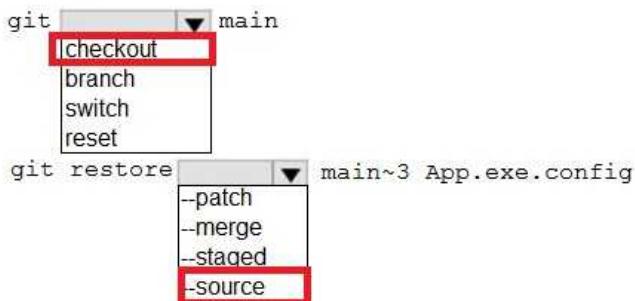
NOTE: Each correct selection is worth one point.

## Answer Area



**Answer:**

## Answer Area



**Explanation:**

Checkout

source

**HOTSPOT**

You company uses a Git source-code repository.

You plan to implement GitFlow as a workflow strategy.

You need to identify which branch types are used for production code and preproduction code in the strategy.

Which branch type should you identify for each code type? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Production code:

A dropdown menu with a light gray header bar containing the text "Production code:" on the left and a black downward-pointing arrow on the right. The menu is open, showing three options: "Main", "Feature", and "Develop".

- Main
- Feature
- Develop

Preproduction code:

A dropdown menu with a light gray header bar containing the text "Preproduction code:" on the left and a black downward-pointing arrow on the right. The menu is open, showing three options: "Main", "Feature", and "Develop".

- Main
- Feature
- Develop

**Answer:**

**Answer Area**

Production code:

A dropdown menu with a light gray header bar containing the text "Production code:" on the left and a black downward-pointing arrow on the right. The menu is open, showing three options: "Main", "Feature", and "Develop". The option "Main" is highlighted with a red rectangular border.

- Main
- Feature
- Develop

Preproduction code:

A dropdown menu with a light gray header bar containing the text "Preproduction code:" on the left and a black downward-pointing arrow on the right. The menu is open, showing three options: "Main", "Feature", and "Develop". The option "Develop" is highlighted with a red rectangular border.

- Main
- Feature
- Develop

## Question: 208

CertyIQ

DRAG DROP

You have an Azure Repos repository named repo1.

You need to clone repo1. The solution must clone only a directory named src/web.

How should you complete the script? To answer, drag the appropriate values to the correct targets. 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                                                     |
|--------------------------------------------------------------------|-----------------------------------------------------------------|
| <code>https://dev.azure.com/organization/project/_git/repo1</code> | ...                                                             |
| <code>git@ssh.dev.azure.com:v3/organization/project/repo1</code>   | <code>cd repos</code>                                           |
| <code>repo1/src</code>                                             | <code>scalar clone</code> <input type="text"/> Value            |
| <code>src/web</code>                                               | <code>cd</code> <input type="text"/> Value                      |
| <code>repo1/src/web</code>                                         | <code>git sparse-checkout set</code> <input type="text"/> Value |
| <code>web</code>                                                   | ...                                                             |

### Answer:

Answer Area

```
...
cd repos
scalar clone https://dev.azure.com/organization/project/_git/repo1
cd repo1/src
git sparse-checkout set web
...
```

### Explanation:

[https://dev.azure.com/ms-scalar/\\_git/scalar](https://dev.azure.com/ms-scalar/_git/scalar)\$ cd scalar/src

## Question: 209

CertyIQ

You use GitHub for source control and Microsoft Teams for collaboration.

You need to send a notification to a Teams channel for each commit. The solution must minimize development effort.

What should you do?

- A. Use Azure Automation to connect to the GitHub Actions API and send a message to the Teams channel.

B.Use the Microsoft Teams for GitHub app and configure a subscription to receive notifications in the Teams channel.

C.Use GitHub Actions with a dispatch to send a message to the Teams channel by using the Teams API.

D.Use Azure Functions to connect to the GitHub REST API and send a message to the Teams channel.

**Answer: B**

**Explanation:**

B is the answer.

<https://github.com/integrations/microsoft-teams#customize-notifications> You can customize your notifications by subscribing to activity that is relevant to your Teams channel, and unsubscribing from activity that is less helpful to your project. Below features are enabled by default, and can be disabled with the @github unsubscribe owner/repo [feature] command:- commits - New commits on the default branch (usually main)

## Question: 210

CertyIQ

DRAG DROP

You have a GitHub repository named repo1.

You migrate repo1 to an Azure Repos repository named repo2.

After the migration, changes are made to repo1.

You need to sync the changes to repo2.

How should you complete the script? To answer, drag the appropriate values to the correct targets. 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

- repo1
- repo1 clone URL
- repo1 repo URL
- repo2
- repo2 clone URL
- repo2 repo URL

### Answer Area

```
...
git clone --bare [REPO1_CLONE_URL]
cd [REPO2_DIR]
git remote add --mirror=fetch upstream [REPO1_REPO_URL]
git fetch upstream --tags
git push origin --all
...
```

**Answer:**

**Values**

|                 |
|-----------------|
| repo1           |
| repo1 clone URL |
| repo1 repo URL  |
| repo2           |
| repo2 clone URL |
| repo2 repo URL  |

**Answer Area**

```
...
git clone --bare [repo2 clone URL]
cd [repo2]
git remote add --mirror=fetch upstream
git fetch upstream --tags
git push origin --all
...
```

**Explanation:**

1. repo2\_clone\_url
2. repo2
3. repo1\_clone\_url

**CertyIQ****Question: 211**

DRAG DROP

You have an Azure Repos repository named repo1.

You delete a branch named features/feature11.

You need to recover the deleted branch.

Which three commands should you 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

|                               |
|-------------------------------|
| git restore <SHA1>            |
| git stash                     |
| git checkout <SHA1>           |
| git branch features/feature11 |
| git log                       |

**Answer Area**

- 1
- 2
- 3

**Answer:**

Commands

|                               |
|-------------------------------|
| git restore <SHA1>            |
| git stash                     |
| git checkout <SHA1>           |
| git branch features/feature11 |
| git log                       |

**Answer Area**

- 1 git log
- 2 git checkout <SHA1>
- 3 git branch features/feature11

**Explanation:**

git log git checkout <SHA1>git branch features/feature11

**CertyIQ****Question: 212**

You use GitHub to host container packages that use Semantic Versioning (SemVer).

You have an app named App1. The current version of App1 is 11.2.0.

You change the code of App1 to fix a bug that was introduced in version 10.5.1.

Which version number should you assign to the release?

A.10.5.1-PATCH

**B.11.2.1**

C.10.5.2

D.10.6.0

**Answer: B**

**Explanation:**

B is the answer.

<https://semver.org/#summary>  
Given a version number MAJOR.MINOR.PATCH, increment the:-  
MAJOR version when you make incompatible API changes- MINOR version when you add functionality in a backward compatible manner- PATCH version when you make backward compatible bug fixes

**Question: 213**

**CertyIQ**

DRAG DROP

You have an Azure Repos repository that contains large PSD files.

You need to configure Git LFS to manage all the files.

How should you complete the script? To answer, drag the appropriate values to the correct targets. 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**

git fetch

git lfs config add "\*.psd"

git lfs migrate import --include=".psd" --everything

git lfs track "\*.psd"

git lfs update

git push

**Answer Area**

...

git lfs install

git add .gitattributes

git commit -m "track \*.psd files using Git LFS"

...

**Answer:**

## Answer Area

```
...
git lfs install
git lfs track "*.psd"
git add .gitattributes
git commit -m "track *.psd files using Git LFS"
git lfs migrate import --include=".psd" --everything
git push
```

### Explanation:

<https://docs.github.com/en/repositories/working-with-files/managing-large-files/configuring-git-large-file-storage>  
<https://github.com/git-lfs/git-lfs/wiki/Tutorial#migrating-existing-repository-data-to-lfs>

## Question: 214

CertyIQ

You manage code by using GitHub.

You need to ensure that repository owners are notified if a new vulnerable dependency or malware is found in their repository.

What should you do?

- A.Configure CodeQL scanning actions.
- B.Configure Dependabot alerts.**
- C.Configure branch protection rules for each repository.
- D.Subscribe all the repository owners to the GitHub Advisory Database.

### Answer: B

### Explanation:

B is the answer.

<https://docs.github.com/en/code-security/dependabot/dependabot-alerts/about-dependabot-alerts>  
Dependabot alerts tell you that your code depends on a package that is insecure. If your code depends on a package with a security vulnerability, this can cause a range of problems for your project or the people who use it. You should upgrade to a secure version of the package as soon as possible. If your code uses malware, you need to replace the package with a secure alternative.

## Question: 215

CertyIQ

You have a public GitHub repository named Public1.

A commit is made to Public1. The commit contains a pattern that matches a regular expression.

Who is notified first when the commit is made?

- A.the administrator of the GitHub organization
- B.the committer
- C.the owner of Public1

D.the secret scanning partner

**Answer: D**

**Explanation:**

D is the answer.

<https://docs.github.com/en/code-security/secret-scanning/about-secret-scanning#about-secret-scanning-alerts-for-partners>When you make a repository public, or push changes to a public repository, GitHub always scans the code for secrets that match partner patterns. Public packages on the npm registry are also scanned. If secret scanning detects a potential secret, we notify the service provider who issued the secret. The service provider validates the string and then decides whether they should revoke the secret, issue a new secret, or contact you directly. Their action will depend on the associated risks to you or them. You cannot change the configuration of secret scanning for partner patterns on public repositories.

**Question: 216**

CertyIQ

You manage source code control and versioning by using GitHub.

A large file is committed to a repository accidentally.

You need to reduce the size of the repository. The solution must remove the file from the repository.

What should you use?

A.bfg

B.lfs

C.gvfs

D.init

**Answer: A**

**Explanation:**

bfg is a correct answer.

**Question: 217**

CertyIQ

Your company has 60 developers who are assigned to four teams. Each team has 15 members.

The company uses an agile development methodology.

You need to structure the work of the development teams so that each team owns their respective work while working together to reach a common goal.

Which parts of the taxonomy should you enable the team to perform autonomously?

A. Features and Tasks

B. Initiatives and Epics

C. Epics and Features

D. Stories and Tasks

**Answer: D**

**Explanation:**

Epics consist of Features, which consist of User Stories, which consist of Tasks.

We want them to work together (on Epics and Features) and enable them to work autonomously (on User Stories and Tasks).

### Question: 218

CertyIQ

Your company creates a new Azure DevOps team.  
You plan to use Azure DevOps for sprint planning.  
You need to visualize the flow of your work by using an agile methodology.  
Which Azure DevOps component should you use?

- A. Kanban boards
- B. sprint planning
- C. delivery plans
- D. portfolio backlogs

### Answer: A

#### Explanation:

Customizing Kanban boards.

To maximize a team's ability to consistently deliver high quality software, Kanban emphasize two main practices. The first, visualize the flow of work, requires you to map your team's workflow stages and configure your Kanban board to match. Your Kanban board turns your backlog into an interactive signboard, providing a visual flow of work.

Reference:

<https://azuredevopslabs.com/labs/azuredevops/agile/>

### Question: 219

CertyIQ

Your company implements an Agile development methodology.  
You plan to implement retrospectives at the end of each sprint.  
Which three questions should you include? Each correct answer presents part of the solution.  
NOTE: Each correct selection is worth one point.

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

### Answer: CDE

#### Explanation:

- C. What could have gone better?
- D. What went well?
- E. What should we try next?

## Question: 220

CertyIQ

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 without forking
- B. multiple long-running branches
- C. a single fork per team member
- D. a single long-running branch with multiple short-lived feature branches

### Answer: D

#### Explanation:

Topic/feature 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>

## Question: 221

CertyIQ

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

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

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

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

Solution: You 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.

## Question: 222

CertyIQ

You have a project in Azure DevOps that has a release pipeline.

You need to integrate work item tracking and an Agile project management system to meet the following requirements:

- ⇒ Ensure that developers can track whether their commits are deployed to production.
  - ⇒ Report the deployment status.
  - ⇒ Minimize integration effort.
- Which system should you use?

- A. Asana
- B. Basecamp
- C. Trello
- D. Jira

**Answer: D**

**Explanation:**

Jira Software is a development tool used by agile teams to plan, track, and manage software releases. Using Azure Pipelines, teams can configure CI/CD pipelines for applications of any language, deploying to any platform or any cloud.

Note: Microsoft and Atlassian have partnered together to build an integration between Azure Pipelines and Jira Software.

This integration connects the two products, providing full tracking of how and when the value envisioned with an issue is delivered to end users. This enables teams to setup a tight development cycle from issue creation through release. Key development milestones like builds and deployments associated to a Jira issue can then be tracked from within Jira Software.

Incorrect Answers:

C: Trello is a collaboration tool that organizes your projects into boards. In one glance, Trello tells you what's being worked on, who's working on what, and where something is in a process.

Reference:

<https://devblogs.microsoft.com/devops/azure-pipelines-integration-with-jira-software/>

**Question: 223**

**CertyIQ**

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. Github Codespaces

**Answer: D**

**Explanation:**

You can develop in your codespace directly in Visual Studio Code by connecting the GitHub Codespaces extension with your account on GitHub.

Reference:

<https://docs.github.com/en/codespaces/developing-in-codespaces/using-codespaces-in-visual-studio-code>

## Question: 224

CertyIQ

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

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

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

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

Solution: You 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.

Reference:

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

## Question: 225

CertyIQ

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

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

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

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

Solution: You 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.

The code push event is triggered when the code is pushed to a Git repository.

Reference:

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

## Question: 226

CertyIQ

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

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

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

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

Solution: You add a trigger to the build pipeline.

Does this meet the goal?

A. Yes

B. No

**Answer: B**

**Explanation:**

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

Reference:

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

**Question: 227**

CertyIQ

You plan to create in Azure DevOps. Multiple developers will work on the project. The developers will work offline frequently and will require access to the full project history while they are offline.

Which version control solution should you use?

A. Team Foundation Version Control

B. Git

C. TortoiseSVN

D. Subversion

**Answer: B**

**Explanation:**

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

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

Incorrect Answers:

A: Team Foundation Version Control: File history is not replicated on the client dev machine and so can be viewed only when you're connected to the server.

Reference:

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

**Question: 228**

CertyIQ

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-vscode>

**CertyIQ**

**Question: 229**

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

**Answer: D**

**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](https://orgName / project_name / _settings/serviceHooks)
2. 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>

**CertyIQ**

**Question: 230**

You have an Azure DevOps organization named Contoso and an Azure subscription.

You use Azure DevOps to build and deploy a web app named App1. Azure Monitor is configured to generate an email notification in response to alerts generated whenever App1 generates a server-side error.

You need to receive notifications in Microsoft Teams whenever an Azure Monitor alert is generated. Which two actions should you perform? Each correct answer presents part of the solution.  
NOTE: Each correct selection is worth one point.

- A. Create an Azure Monitor workbook.
- B. Create an Azure logic app that has an HTTP request trigger.
- C. Create an Azure logic app that has an Azure DevOps trigger.
- D. Modify an action group in Azure Monitor.
- E. Modify the Diagnostics settings in Azure Monitor.

**Answer: BD**

**Explanation:**

In Azure Monitor action group configure a webhook, the url of the webhook must be the url (trigger) of the Logic App. In the Logic App you can use the Team connector to send a message to a Teams channel

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups-logic-app>

### Question: 231

CertyIQ

HOTSPOT -

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.

Hot Area:

### Answer Area

|               |                          |                          |
|---------------|--------------------------|--------------------------|
| /azrepos      | <input type="checkbox"/> | <input type="checkbox"/> |
| feedback      | <input type="checkbox"/> | <input type="checkbox"/> |
| signin        | <input type="checkbox"/> | <input type="checkbox"/> |
| subscribe     | <input type="checkbox"/> | <input type="checkbox"/> |
| subscriptions | <input type="checkbox"/> | <input type="checkbox"/> |

**Answer:**

## Answer Area



### Explanation:

Box 1: subscribe -

To start monitoring all Git repositories in a project, use the following slash command inside a channel:

/azrepos subscribe [project url]

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

You can also monitor a specific repository using the following command:

/azrepos subscribe [repository url]

The repository URL can be to any page within your repository that has your repository name.

For example, for Git repositories, use:

/azrepos subscribe https://dev.azure.com/myorg/myproject/\_git/myrepository

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/integrations/repos-slack>

CertyIQ

## Question: 232

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

You need to create a published wiki in Project1.

What should you do first?

- A. Modify the Storage settings of Project1.
- B. In Project1, create an Azure DevOps pipeline.
- C. In Project1, create an Azure DevOps repository.**
- D. Modify the Team configuration settings of Project1.

Answer: C

### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/devops/project/wiki/publish-repo-to-wiki?view=azure-devops&tabs=broser>

CertyIQ

## Question: 233

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.

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

Reference:

<https://searchunifiedcommunications.techtarget.com/definition/Microsoft-Teams>

**Question: 234**

**CertyIQ**

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

The application will use Azure functions to write some data to Azure Storage.

You need to send the Azure DevOps team an email message when the front end fails to return a status code of 200. Which feature should you use?

- A. Service Map in Azure Log Analytics
- B. availability tests in Azure Application Insights
- C. Profiler in Azure Application Insights
- D. Application Map in Azure Application Insights

**Answer: B**

**Explanation:**

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.

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

**Question: 235**

**CertyIQ**

You have a project in Azure DevOps named Project1. Project1 contains a published wiki.

You need to change the order of pages in the navigation pane of the published wiki in the Azure DevOps portal. What should you do?

- A. At the root of the wiki, create a file named .order that defines the page hierarchy.

- B. At the root of the wiki, create a file named wiki.md that defines the page hierarchy.
- C. Rename the pages in the navigation pane.
- D. Drag and drop the pages in the navigation pane.

**Answer: A**

**Explanation:**

"To structure the list of pages in the navigation pane for a \*publish code as wiki\*, define the .order file at the root, and for each subfolder or parent page that contains subpages."

"The \*provisioned\* wiki manages the page sequence and page list automatically as you add or move pages within the navigation pane."

<https://docs.microsoft.com/en-us/azure/devops/project/wiki/provisioned-vs-published-wiki?view=azure-devops#page-sequence-and-page-list-in-navigation-pane>

**Question: 236**

**CertyIQ**

DRAG DROP -

You have a GitHub organization named org1 and an Azure tenant named Tenant1.

You need to enable single sign-on (SSO) in Azure Active Directory (Azure AD) for the users in org1.

Which URIs should you use for the SAML configuration in Azure AD? To answer, drag the appropriate URIs to the correct settings. Each URI may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

**URIs**

<https://github.com/orgs/org1>

<https://github.com/orgs/org1/sso>

<https://login.microsoftonline.com/tenant1>

<https://github.com/orgs/org1/saml/consume>

<https://login.microsoftonline.com/tenant1.com>

**Answer Area**

Identifier (Entity ID):

Reply URL (Assertion Consumer Service URL):

Sign on URL:

**Answer:**

**URIs**

<https://github.com/orgs/org1>

<https://github.com/orgs/org1/sso>

<https://login.microsoftonline.com/tenant1>

<https://github.com/orgs/org1/saml/consume>

<https://login.microsoftonline.com/tenant1.com>

**Answer Area**

Identifier (Entity ID):

<https://github.com/orgs/org1>

Reply URL (Assertion Consumer Service URL):

<https://github.com/orgs/org1/saml/consume>

Sign on URL:

<https://github.com/orgs/org1/sso>

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/github-tutorial>

**Question: 237**

CertyIQ

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. Skype for Business
- B. Bamboo
- C. Octopus
- 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.

Reference:

<https://marketplace.visualstudio.com/items?itemName=ms-vsts.vss-services-slack>

**Question: 239**

CertyIQ

You have a pipeline named Pipeline1 in Azure Pipelines.

You need to create a service connection to enable Pipeline1 to download a public container image.

Which type of service connection should you create?

- A. a Docker host
- B. a Docker registry
- C. Azure Service Fabric
- D. Azure Kubernetes Service (AKS)

**Answer: B****Explanation:**

Reference:

**Question: 240**

You have a project in Azure DevOps named Project1 that contains a Kanban board named Board1.

You create a Microsoft Teams channel and add the Azure Boards app to the channel.

You need to ensure that users can create work items in Board1 from Microsoft Teams.

Which command should you run?

- A. @azure boards subscriptions
- B. @azure boards create
- C. @azure boards sign in
- D. **@azure boards link**

**Answer: D**

**Explanation:**

After signing in, use the following command inside a Teams channel to link to the Azure Boards project that you specify with the URL:

@azure boards link [project url]

Once the project is linked, you can create work items using @azure boards create command or use message actions.

<https://learn.microsoft.com/en-us/azure/devops/boards/integrations/boards-teams?view=azure-devops>

**Question: 241**

You manage a project by using Azure Board, and you manage the project code by using Azure Repos.

You have a bug work item that has an ID of 123.

You need to set the work item state to Resolved.

What should you add to the commit message?

- A. #123 completes
- B. #123 Resolved
- C. Completed #123
- D. Fixes #123

**Answer: D**

**Explanation:**

<https://learn.microsoft.com/en-us/azure/devops/boards/github/link-to-from-github?view=azure-devops#use-ab-mention-to-link-from-github-to-azure-boards-work-items>

## Question: 242

CertyIQ

You have an Azure subscription that contains a storage account and 20 virtual machines.

You plan to use LogRhythm for aggregation and analysis of the virtual machine logs.

You need to configure AzLog to export the logs and push them to the storage account.

In which format should you export the logs?

- A. JSON
- B. EVTX
- C. EVT
- D. binary

### Answer: A

#### Explanation:

The LogRhythm Open Collector brings modern logs, usually in JSON format, from cloud log sources, flat file, or other formats, into the LogRhythm SIEM. It is designed for easy mapping of JSON fields to the LogRhythm Schema Dictionary and Guide.

## Question: 243

CertyIQ

DRAG DROP

You use Exabeam Fusion SIEM and the Azure cloud platform.

You need to integrate Exabeam and Azure. The solution must use OAuth 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

Upload a certificate.

Create a client secret.

Register an Exabeam application in Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra.

Configure the Exabeam Azure cloud connector.

Configure API permissions.



#### Answer:

## Actions

Upload a certificate.

Create a client secret.

Register an Exabeam application in Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra.

Configure the Exabeam Azure cloud connector.

Configure API permissions.

## Answer Area



1 Register an Exabeam application in Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra.

2 Configure the Exabeam Azure cloud connector.

3 Configure API permissions.



### Explanation:

Register oauth (ad)

Configure connector

Configure API

## Question: 244

CertyIQ

You use GitHub for source control and Azure Boards for project management. GitHub and Azure Boards are integrated.

You plan to create a pull request in GitHub.

You need to automatically link the request to an existing Azure Boards work item by using the text of AB#.

To which two elements can you add the text? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. milestone
- B. label
- C. title
- D. comment
- E. description

### Answer: CE

### Explanation:

<https://learn.microsoft.com/en-us/azure/devops/boards/github/link-to-from-github?view=azure-devops#:~:text=within%20the%20title%20or%20description>

**HOTSPOT**

You are using Agile process methodologies in Azure DevOps.

You need to deploy a dashboard that will provide progress reports for the following work items:

- How long it took to close a work item after it was created.
- How long it took to close a work item after the work was started.

Which type of widget should you use for each work item? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

How long it took close a work item after it was created:

- Burndown chart
- Cumulative flow diagram
- Cycle time
- Lead time
- Velocity

How long it took to close a work item after the work was started:

- Burndown chart
- Burnup chart
- Cycle time
- Lead time
- Velocity

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

How long it took close a work item after it was created:

- Burndown chart
- Cumulative flow diagram
- Cycle time
- Lead time**
- Velocity

How long it took to close a work item after the work was started:

- Burndown chart
- Burnup chart
- Cycle time**
- Lead time
- Velocity

**Explanation:**

## 1. Lead time2. Cycle time

<https://learn.microsoft.com/en-us/azure/devops/report/dashboards/cycle-time-and-lead-time?view=azure-devops> Both lead time and cycle time widgets are useful to teams. They both indicate how long it takes for work to flow through their development pipeline. Lead time measures the total time elapsed from the creation of work items to their completion. Cycle time measures the time it takes for your team to complete work items once they begin actively working on them.

CertyIQ

### Question: 246

You are integrating an Azure Boards project and a GitHub repository.

You need to authenticate Azure Boards to GitHub.

Which two authentication methods can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A.a publisher certificate
- B.a trusted root certificate
- C.Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
- D.GitHub user credentials
- E.a personal access token (PAT)

### Answer: DE

#### Explanation:

DE is the answer.

<https://learn.microsoft.com/en-us/azure/devops/boards/github/connect-to-github?view=azure-devops#authentication-options> The following authentication options are supported based on the GitHub platform you want to connect to. GitHub.com- GitHub.com user account (Recommended)- Personal access token (PAT)

CertyIQ

### Question: 247

You have a GitHub repository that is integrated with Azure Boards. Azure Boards has a work item that has the number 715.

You need to ensure that when you commit source code in GitHub, the work item is updated automatically.

What should you include in the commit comments?

- A.the URL of the work item
- B.AB#715
- C.@715
- D.#715

### Answer: B

#### Explanation:

B is the answer.

<https://learn.microsoft.com/en-us/azure/devops/boards/github/link-to-from-github?view=azure-devops#use-ab-mention-to-link-from-github-to-azure-boards-work-items>From a GitHub commit, pull request or issue, use the following syntax to create a link to your Azure Boards work item. Enter the AB#ID within the text of a commit message. Or, for a pull request or issue, enter the AB#ID within the title or description (not a comment).

CertyIQ

### Question: 248

You are creating a dashboard in Azure Boards.

You need to visualize the time from when work starts on a work item until the work item is closed.

Which type of widget should you use?

- A.cycle time
- B.velocity
- C.cumulative flow
- D.lead time

**Answer: A**

**Explanation:**

A is the answer.

<https://learn.microsoft.com/en-us/azure/devops/report/dashboards/cycle-time-and-lead-time?view=azure-devops>Both lead time and cycle time widgets are useful to teams. They both indicate how long it takes for work to flow through their development pipeline. Lead time measures the total time elapsed from the creation of work items to their completion. Cycle time measures the time it takes for your team to complete work items once they begin actively working on them.

CertyIQ

### Question: 249

You manage a project by using Azure Boards. You manage the project code by using GitHub.

You have three work items that have IDs of 456, 457, and 458.

You need to create a pull request that will be linked to all the work items. The solution must set the state of work item 456 to done.

What should you add to the commit message?

- A.Fixes #456, #457, #458
- B.Fixes #AB456, #AB457, #AB458
- C.#456, #457, #458  
Completed #456
- D.#AB456, #AB457, #AB458

**Answer: A**

**Explanation:**

The correct answer is A. We just need to reference the workitems using "#ID". To close a workitem we can use the syntax "Fixes #ID". Multiple workitems can be referenced being divided by a ",".

### Question: 250

CertyIQ

You manage code by using GitHub.

You plan to ensure that all GitHub Actions are validated by a security team.

You create a branch protection rule requiring that code changes be reviewed by code owners.

You need to create the CODEOWNERS file.

Where should you create the file?

- A..github/actions/
- B..github/**
- C..git/
- D..github/workflows/

### Answer: B

#### Explanation:

..github/

<https://docs.github.com/es/repositories/managing-your-repositorys-settings-and-features/customizing-your-repository/about-code-owners>

### Question: 251

CertyIQ

You manage a project by using Azure Boards. You manage the project code by using GitHub.

You have three work items that have IDs of 456, 457, and 458.

You need to create a pull request that will be linked to all the work items. The solution must set the state of work item 456 to done.

What should you add to the commit message?

- A.Done #456, #457, #458
- B.#AB456, #AB457, #AB458
- C.#456, #457, #458  
Completed #456
- D.#AB456, #AB457, #AB458  
Completed #AB456**

### Answer: D

#### Explanation:

for GitHub, should use AB# notation and "Completed" keyword to change the status of the work item.

## Question: 252

CertyIQ

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 build 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 the Windows Server 2019 with Visual Studio 2019 image. Include the Java Tool

Installer task in the build pipeline.

Does this meet the goal?

A. Yes

B. No

### Answer: B

#### Explanation:

We need a self host agent, Microsoft's agents can not access to On-premise resources.

## Question: 253

CertyIQ

You have a project in Azure DevOps.

You create the following YAML template named Template1.yml.

steps:

- script: npm install
- script: yarn install
- script: npm run compile

You create the following pipeline named File1.yml.

parameters:

- usersteps:
- task: [email protected]
  - script: echo Done

You need to ensure that Template1.yaml runs before File1.yml.

How should you update File1.yml?

- A. parameters: usersteps: extends: template: template1.yml - task: [email protected] - script: echo Done
- B. template: template1.yml parameters: usersteps: - task: [email protected] - script: echo Done
- C. extends: template: template1.yml parameters: usersteps: - task: [email protected] - script: echo Done
- D. parameters: usersteps: - template: template1.yml - task: [email protected] - script: echo Done

### Answer: C

#### Explanation:

Azure Pipelines offers two kinds of templates: includes and extends. Included templates behave like #include in C++: it's as if you paste the template's code right into the outer file, which references it. To continue the C++ metaphor, extends templates are more like inheritance: the template provides the outer structure of the pipeline and a set of places where the template consumer can make targeted alterations.

Example:

extends:

template: [email protected]

```
parameters:
usersteps:
- script: echo This is my first step
- script: echo This is my second step
```

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/security/templates>

CertyIQ

### Question: 254

You have an Azure solution that contains a build pipeline in Azure Pipelines.

You experience intermittent delays before the build pipeline starts.

You need to reduce the time it takes to start the build pipeline.

What should you do?

- A. Enable self-hosted build agents.
- B. Create a new agent pool.
- C. Split the build pipeline into multiple stages.
- D. Purchase an additional parallel job.

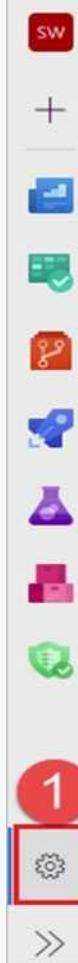
### Answer: D

#### Explanation:

We need to ensure that resources are available without a startup delay. We don't have enough concurrency.

To check how much concurrency you have:

To check your limits, navigate to Project settings, Parallel jobs.



## Project Settings

Space Game - web

### General

[Overview](#)[Teams](#)[Permissions](#)[Notifications](#)[Service hooks](#)[Dashboards](#)

### Boards

[Project configuration](#)[Team configuration](#)[GitHub connections](#)

### Pipelines

[Agent pools](#)[Parallel jobs](#)[Settings](#)

### Private projects



Microsoft-hosted ⓘ

[View in-progress jobs](#)

Free tier

1 parallel job up to 50000 mins/mo

[Purchase parallel jobs](#)

Self-hosted ⓘ

[View in-progress jobs](#)

Unlimited

Parallel jobs



Free parallel jobs

Unlimited



Visual Studio Enterprise subscribers ⓘ

0



Monthly purchases

0 [Change](#)

### Public projects Free



Microsoft-hosted ⓘ

10

Parallel jobs



Self-hosted ⓘ

[View in-progress jobs](#)

Unlimited

Parallel jobs

Reference:

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

## Question: 255

CertyIQ

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 build 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

### Explanation:

You cannot use Microsoft-hosted agents or the Azure Pipelines agent pool with on-premises TFS or Azure

DevOps Server.

<https://docs.microsoft.com/bs-latn-ba/azure/devops/pipelines/agents/hosted?view=azure-devops-2020&tabs=yaml>

### Question: 256

CertyIQ

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>

### Question: 257

CertyIQ

DRAG DROP -

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.

Select and Place:

## 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:

Project2:

Project3:

## Explanation:

Project1: Git in Azure Repos -

Project2: GitHub Enterprise -

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

Project3: assembla Subversion

## Question: 258

CertyIQ

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: B

#### Explanation:

The right approach should be and always be around Azure. The key point is the on-premises dependency management system. In Azure, the self-host build agent is designed for this purpose. The self-host agent is in the default agent pool. The rest of requirements could be done in ADO. So the answer is NO.

### Question: 259

CertyIQ

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: A

#### Explanation:

I have experienced in these types of questions where answer is - Yes / NO - and you can not go back - as you can get the clue - right answer i.e. " Yes " is the last questions usually :-)

### Question: 260

CertyIQ

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

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

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

the following requirements:

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

Solution: Configure the build pipeline to use a Hosted VS 2019 agent pool. Include the Java Tool Installer task in the build pipeline.

Does this meet the goal?

A. Yes

B. No

**Answer: B**

**Explanation:**

Instead use Octopus Tentacle.

Reference:

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

## Question: 261

CertyIQ

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: B**

**Explanation:**

Instead use Octopus Tentacle.

Reference:

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

## Question: 262

CertyIQ

Your company uses a Git repository in Azure Repos to manage the source code of a web application. The master branch is protected from direct updates.

Developers work on new features in the topic branches.

Because of the high volume of requested features, it is difficult to follow the history of the changes to the master branch.

You need to enforce a pull request merge strategy. The strategy must meet the following requirements:

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

Which merge strategy should you use in the branch policy?

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

**Answer: A**

**Explanation:**

Squash merging is a merge option that allows you to condense the Git history of topic branches when you complete a pull request. Instead of each commit on the topic branch being added to the history of the default branch, a squash merge takes all the file changes and adds them to a single new commit on the default branch.

A simple way to think about this is that squash merge gives you just the file changes, and a regular merge gives you the file changes and the commit history.

Note: Squash merging keeps your default branch histories clean and easy to follow without demanding any workflow changes on your team. Contributors to the topic branch work how they want in the topic branch, and the default branches keep a linear history through the use of squash merges. The commit history of a master branch updated with squash merges will have one commit for each merged branch. You can step through this history commit by commit to find out exactly when work was done.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/merging-with-squash>

**Question: 263**

**CertyIQ**

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 selection is worth one point.

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

**Answer: BDE**

**Explanation:**

B: Jenkins requires a plug-in to connect to TFS and check for updates to a project.

Jenkins' built-in Git Plugin or Team Foundation Server Plugin can poll a Team Services repository every few minutes and queue a job when changes are detected.

D: After you have generated credentials using Visual Studio Team Services, you need to use those credentials in Jenkins.

E. Create a service hook in Azure DevOps.

**Question: 264**

**CertyIQ**

**DRAG DROP -**

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 on the server before merging any changes to the main branch: <ul style="list-style-type: none"><li>• Changes must be reviewed by at least two project members.</li><li>• Changes must be associated by at least one work item</li></ul> |
| 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.

Select and Place:

**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: Git                             |
| Subversion                      | Project 3: Git                             |
| Team Foundation Version Control | Project 4: Team Foundation Version Control |

### Explanation:

Box 1: Team Foundation Version Control

TFVC lets you apply granular permissions and restrict access down to a file level.

Box 2: Git -

Git is the default version control provider for new projects. You should use Git for version control in your projects unless you have a specific need for centralized version control features in TFVC.

Box 3: git

Box 4: team foundation version control

### Question: 265

CertyIQ

You are automating the build process for a Java-based application by using Azure DevOps. You need to add code coverage testing and publish the outcomes to the pipeline. What should you use?

- A. Bullseye Coverage
- B. JUnit
- C. JaCoCo**
- D. MSTest

### Answer: C

#### Explanation:

Use Publish Code Coverage Results task in a build pipeline to publish code coverage results to Azure Pipelines or TFS, which were produced by a build in Cobertura or JaCoCo format.

Incorrect Answers:

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

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

⇒ Cobertura

⇒ JaCoCo

Other incorrect answer options you may see on the exam include the following:

⇒ Coverlet

⇒ NUnit

⇒ Coverage.py

Reference:

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

## Question: 266

CertyIQ

HOTSPOT -

Your 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.

The screenshot shows the Azure DevOps web interface. On the left, the sidebar has 'Fast Track' selected under 'Pipelines'. The main area shows 'Jobs in run #20191120.1' for the 'Fast Track' pipeline. The 'initial\_build' job is expanded, showing its steps: 'initialize build' (7s), which includes 'Initialize job' (<1s), 'Checkout' (4s), 'CmdLine' (2s), 'Post-job: Ccheckout' (<1s), and 'Finalize Job' (<1s). Below this are collapsed sections for 'deploy\_to\_dev' (2s), 'deploy\_to\_uat' (2s), and 'Finalize build' (<1s). A callout box highlights the 'initial\_build' job with the following details:

|   |                              |
|---|------------------------------|
| 1 | <u>Pool: Azure Pipelines</u> |
| 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.

Hot Area:

## Answer Area

The pipeline contains

|              |   |
|--------------|---|
|              | ▼ |
| one stage    |   |
| two stages   |   |
| three stages |   |
| four stages  |   |
| five stages  |   |

Build\_vm contains

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

Answer:

## Answer Area

The pipeline contains

|              |   |
|--------------|---|
|              | ▼ |
| one stage    |   |
| two stages   |   |
| three stages |   |
| four stages  |   |
| five stages  |   |

Build\_vm contains

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

Explanation:

3stage

1 Job

DRAG DROP -

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.

Select and Place:

## Build Agent Pools

## Answer Area

Hosted Windows Container

Hosted Linux

Hosted macOS

Hosted

Default

An application that runs on iOS:

An Internet Information Services (IIS) web application that runs in Docker:

Answer:

## Build Agent Pools

## Answer Area

Hosted Windows Container

Hosted Linux

Hosted macOS

Hosted

Default

An application that runs on iOS:

Hosted macOS

An Internet Information Services (IIS) web application that runs in Docker:

Hosted

## Explanation:

Box 1: Hosted macOS -

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

Box 2: Hosted -

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

Incorrect Answers:

Default pool: Use it to register self-hosted agents that you've set up.

Hosted Windows Container pool (Azure Pipelines only): Enabled you to build and release inside Windows containers. Unless you're building using containers,

Windows builds should run in the Hosted VS2017 or Hosted pools.

Hosted Linux/Ubuntu 18.04 does not apply for Mac OS or for Microsoft IIS.

Reference:

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

CertyIQ

### Question: 268

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.

Incorrect Answers:

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

D: If you're building on Linux or macOS, you can use Coverlet or a similar tool to collect code coverage metrics. Code coverage results can be published to the server by using the Publish Code Coverage Results task. To leverage this functionality, the coverage tool must be configured to generate results in Cobertura or JaCoCo coverage format.

F: Coverage.py is used for Python, not for Java.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

- 1. Cobertura
- 2. JaCoCo

Other incorrect answer options you may see on the exam include the following:

- 1. Junit
- 2. NUnit
- 3. Coverage.py

Reference:

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

CertyIQ

### Question: 269

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

### Answer: A

#### 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.

Incorrect Answers:

B: The workspace clean options are applicable only for self-hosted agents. When using Microsoft-hosted agents job are always run on a new agent.

Reference:

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

### Question: 270

CertyIQ

HOTSPOT -

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.

Hot Area:

## Answer Area

App1:

▼

canary

rolling

runonce

App2:

▼

canary

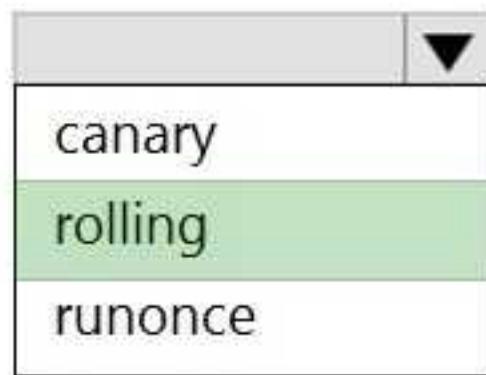
rolling

runonce

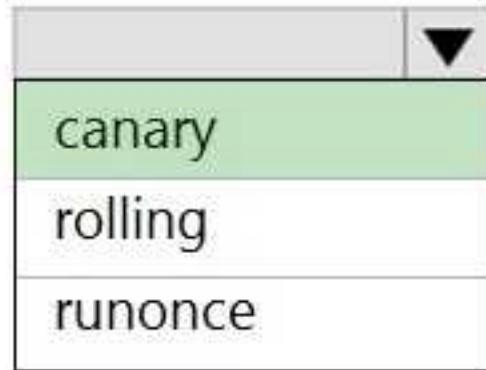
Answer:

## Answer Area

App1:



App2:



### Explanation:

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.

Incorrect Answers:

runonce:

runOnce is the simplest deployment strategy wherein all the lifecycle hooks, namely preDeploy, deploy, routeTraffic, and postRouteTraffic, are executed once.

Then, either on: success or on: failure is executed.

Reference:

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

### Question: 271

CertyIQ

You have a private project in Azure DevOps.

You need to ensure that a project manager can create custom work item queries to report on the project's progress. The solution must use the principle of least privilege.

To which security group should you add the project manager?

- A. Reader
- B. Project Collection Administrators
- C. Project Administrators

## D. Contributor

### Answer: 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.

## Question: 272

CertyIQ

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 2019.

You need to recommend a deployment strategy for the virtual machines. The strategy must meet the following requirements:

- ⇒ Ensure that the virtual machines maintain a consistent configuration.
- ⇒ Minimize administrative effort to configure the virtual machines.

What should you include in the recommendation?

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

### Answer: A

#### Explanation:

It's A: PS DSC. CSE only runs a script and doesn't check for consistency. DSC "Maintains" consistency by regularly checking the target.

## Question: 273

CertyIQ

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. upstream sources
- C. views in Azure Artifacts
- D. a symbol server

### Answer: B

#### Explanation:

Upstream sources enable you to use a single feed to store both the packages you produce and the packages you consume from "remote feeds". This includes both public feeds, such as npmjs.com and nuget.org, and authenticated feeds, such as other Azure DevOps feeds in your organization. Once you've enabled an upstream source, any user connected to your feed can install a package from the remote feed, and your feed will save a copy.

Reference:

<https://azure.microsoft.com/en-us/blog/deep-dive-into-azure-artifacts/>

CertyIQ

### Question: 274

DRAG DROP -

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.

Select and Place:

#### Actions

Create a DSC metaconfiguration

Copy the metaconfiguration to the virtual machines

Add the virtual machines as DSC nodes in Azure Automation

Install Windows Management Framework 5.1 on the virtual machines

From the virtual machines, run `setdsclocalconfigurationmanager.py`

#### Answer Area



#### Answer:

#### Actions

Create a DSC metaconfiguration

Copy the metaconfiguration to the virtual machines

Add the virtual machines as DSC nodes in Azure Automation

Install Windows Management Framework 5.1 on the virtual machines

From the virtual machines, run `setdsclocalconfigurationmanager.py`

#### Answer Area

Create a DSC metaconfiguration

Copy the metaconfiguration to the virtual machines

From the virtual machines, run `setdsclocalconfigurationmanager.py`



#### 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: From the virtual machines, run setdsclocalconfigurationmanager.py

<https://docs.microsoft.com/en-us/azure/automation/automation-dsc-onboarding#enable-physicalvirtual-linux-machines>

## Question: 275

CertyIQ

### SIMULATION -

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 explanation 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.



## SETTINGS

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 | DIRECTORY |
|---------------------------------------------|-------------------------|-----------------------|-----------------|-------|-----------|
| SUBSCRIPTION                                | SUBSCRIPTION ID         | ACCOUNT ADMINISTRATOR |                 |       |           |
| Windows Azure MSDN - Visual Studio Ultimate | [REDACTED]              | [REDACTED]            |                 |       |           |

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.



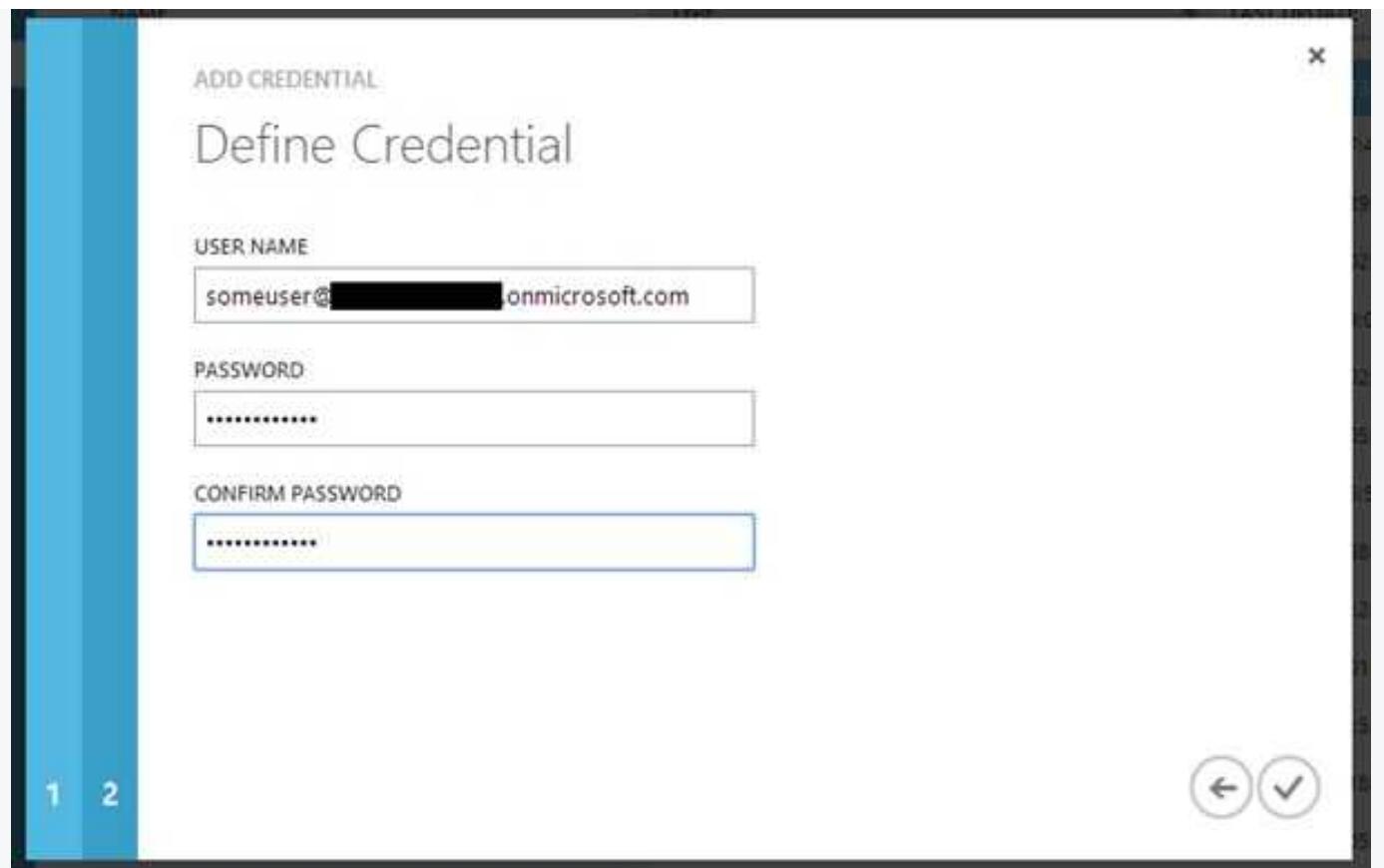
2. Click the directory name that is associated with this Azure subscription.
  3. Click on the Users tab and then click the Add User button.
  4. For type of user, select New user in your organization. Enter a username for the user to create.
  5. Fill out the user's profile. For role, pick User. Don't 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.

Reference:

<https://azure.microsoft.com/sv-se/blog/azure-automation-authenticating-to-azure-using-azure-active-directory/>

### Question: 276

CertyIQ

DRAG DROP -

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

NOTE: Each correct selection is worth one point.

Select and Place:

**Values**

```
dotnet publish -c Release -o out
dotnet restore
mcr.microsoft.com/dotnet/aspnet:5.0
mcr.microsoft.com/dotnet/sdk:5.0
```

**Answer Area**

```
FROM Value AS build-env
COPY . /app/
WORKDIR /app
RUN Value
FROM Value
COPY --from=build-env /app/out /app
WORKDIR /app
ENTRYPOINT ["dotnet", "MvcMovie.dll"]
```

**Answer:**

| Values                           | Anser Area                                         |
|----------------------------------|----------------------------------------------------|
| dotnet publish -c Release -o out | FROM mcr.microsoft.com/dotnet/sdk:5.0 AS build-env |
|                                  | COPY . /app/                                       |
|                                  | WORKDIR /app                                       |
|                                  | RUN dotnet publish -c Release -o out               |
|                                  | FROM mcr.microsoft.com/dotnet/aspnet:5.0           |
|                                  | COPY --from=build-env /app/out /app                |
|                                  | WORKDIR /app                                       |
|                                  | ENTRYPOINT ["dotnet", "MvcMovie.dll"]              |

**Explanation:**

Box 1: mcr.microsoft.com/dotnet/sdk:5.0

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:5.0 comes packaged with the .NET core 5.0 SDK installed, so it's up to the task of building ASP .NET core projects targeting version 5.0

Box 2: DOTNET PUBLISH -C release-o out

RUN dotnet restore -

Box 3: mcr.microsoft.com/dotnet/aspnet:5.0

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 docker file 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/en-us/virtualization/windowscontainers/quick-start/building-sample-app>

**Question: 277****CertyIQ**

DRAG DROP -

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.

Select and Place:

## Answer Area

### 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:

## Answer Area

### Policy Types

A build policy

A check-in policy

A status policy

Committed code must compile successfully:

A build policy

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

A status policy

### Explanation:

Box 1: a build policy

Box 2: a status policy

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

<https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops#build-validation>

## Question: 278

CertyIQ

You use a Git repository in Azure Repos to manage the source code of a web application. Developers commit changes directly to the default branch.

You need to implement a change management procedure that meets the following requirements:

- ⇒ The default 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 default branch by using pull requests.

What should you configure in Azure Repos?

- A. branch policies of the default branch
- B. Services in Project Settings
- C. Deployment pools in Project Settings
- D. branch security of the default 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>

**CertyIQ****Question: 279**

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. Squash merge - creates a linear history with a single commit in the target branch with the changes from the source branch.

**CertyIQ****Question: 280**

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****Explanation:**

YES. Squash merge - creates a linear history with a single commit in the target branch with the changes from the source branch.

## Question: 281

CertyIQ

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>

## Question: 282

CertyIQ

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>

## Question: 283

CertyIQ

You need to recommend a Docker container build strategy that meets the following requirements:

- ⇒ Minimizes image sizes
- ⇒ Minimizes the security surface area of the final image

What should you include in the recommendation?

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

### Answer: A

#### Explanation:

Multi-stage builds are a new feature requiring Docker 17.05 or higher on the daemon and client. Multistage builds are useful to anyone who has struggled to optimize Dockerfiles while keeping them easy to read and maintain.

Incorrect Answers:

C: A swarm consists of multiple Docker hosts which run in swarm mode and act as managers (to manage membership and delegation) and workers (which run swarm services).

Reference:

<https://docs.docker.com/develop/develop-images/multistage-build/>

## Question: 284

CertyIQ

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: 3.1-sdk
02 COPY . /
03 RUN dotnet publish -c Release -o out
04 FROM microsoft/dotnet: 3.1-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:

Correct answer is 4. Final image shall not be sdk but runtime image

## Question: 285

CertyIQ

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 Triggers tab of the build pipeline, you select Batch changes while a build is in progress.

Does this meet the goal?

A. Yes

B. No

### Answer: B

#### Explanation:

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

1. Select the Triggers tab.
2. Enable Continuous integration.

Note: Batch changes -

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

Reference:

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

## Question: 286

CertyIQ

HOTSPOT -

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.

Hot Area:

### Answer Area

Containers must only be published internally:

|                           |
|---------------------------|
| <input type="checkbox"/>  |
| Azure Container Instances |
| Azure Container Registry  |
| Dockerfile                |

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

|                                            |
|--------------------------------------------|
| <input type="checkbox"/>                   |
| An Azure Active Directory (Azure AD) group |
| An Azure Automation account                |
| An Azure service principal                 |

### Answer:

## Answer Area

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:

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.

Reference:

<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>

## Question: 287

CertyIQ

You have 50 Node.js-based projects that you scan by using WhiteSource. Each project includes Package.json, Package-lock.json, and Npm-shrinkwrap.json files.

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

What should you do?

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

### Answer: B

### Explanation:

Separate Your Dependencies -

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

Reference:

<https://blogs.msdn.microsoft.com/visualstudioalmrangers/2017/06/08/manage-your-open-source-usage-and-security-as-reported-by-your-cicd-pipeline/>

**Question: 288****CertyIQ**

Your company deploys applications in Docker containers.  
You want to detect known exploits in the Docker images used to provision the Docker containers.  
You need to integrate image scanning into the application lifecycle. The solution must expose the exploits as early as possible during the application lifecycle.  
What should you configure?

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

**Answer: A****Explanation:**

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

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

**Incorrect Answers:**

C: We should not wait until deployment. We want to detect the exploits as early as possible.

D: We should wait until the image is in the product container. We want to detect the exploits as early as possible.

**Reference:**

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

**Question: 289****CertyIQ**

Your company has a hybrid cloud between Azure and Azure Stack.  
The company uses Azure DevOps for its full CI/CD pipelines. Some applications are built by using Erlang and Hack.  
You need to ensure that Erlang and Hack are supported as part of the build strategy across the hybrid cloud. The solution must minimize management overhead.  
What should you use to execute the build pipeline?

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

**Answer: D****Explanation:**

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

**Reference:**

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

## Question: 290

CertyIQ

Your company has an Azure DevOps project.  
The source code for the project is stored in an on-premises repository and uses 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: DE**

**Explanation:**

When generating the config strict, you have the option to include your PAT automatically

Answer is D and E. Its literally written here - <https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/v2-windows?view=azure-devops>

## Question: 291

CertyIQ

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.  
You are configuring a build pipeline in Azure Pipelines that will include a task named Task1. Task1 will authenticate by using an Azure AD service principal.  
Which three values should you configure for Task1? Each correct answer presents part of the solution.  
NOTE: Each correct selection is worth one point.

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

**Answer: ADC**

**Explanation:**

- A. the tenant ID
- D. the app ID
- C. the client secret

## Question: 292

CertyIQ

DRAG DROP -

You are deploying a new application that uses Azure virtual machines.  
You plan to use the Desired State Configuration (DSC) extension on the virtual machines.  
You need to ensure that the virtual machines always have the same Windows feature installed.

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

Select and Place:

## Actions

Configure the DSC extension on the virtual machines.

Create a YAML configuration file.

Load the file to Azure Blob storage.

Configure the Custom Script Extension on the virtual machines.

Load the file to Azure Files.

Create a PowerShell configuration file.

## Answer Area



### Answer:

#### Actions

Configure the DSC extension on the virtual machines.

Create a YAML configuration file.

Load the file to Azure Blob storage.

Configure the Custom Script Extension on the virtual machines.

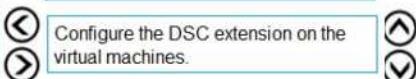
Load the file to Azure Files.

Create a PowerShell configuration file.

#### Answer Area

Create a PowerShell configuration file.

Load the file to Azure Blob storage.



### Explanation:

1. Create a PowerShell configuration file
2. Load the file to Azure Blob storage
3. Configure the \*DSC extension\* on the virtual machines

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

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:**

a multi-stage Docker file

"Build and test with a multi-stage Docker file: 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=trx%2Cyaml>

**Question: 294**

**CertyIQ**

You are designing an Azure DevOps strategy for your company's development team.

You suspect that the team's productivity is low due to accumulate technical debt.

You need to recommend a metric to assess the amount of the team's technical debt.

What should you recommend?

- A. the number of code modules in an application
- B. the number of unit test failures
- C. the percentage of unit test failures
- D. the percentage of overall time spent on rework**

**Answer: D**

**Explanation:**

Technical Debt is the estimated cost to fix code elements issues.

Technical Debt Ratio: Ratio between the cost to develop the software and the cost to fix it. The Technical Debt Ratio formula is:

Remediation cost / Development cost

Which can be restated as:

Remediation cost / (Cost to develop 1 line of code \* Number of lines of code)

Reference:

<http://www.azure365.co.in/devops/3PDevOps-4>

**Question: 295**

**CertyIQ**

You are developing an open source solution that uses a GitHub repository.

You create a new public project in Azure DevOps.

You plan to use Azure Pipelines for continuous build. The solution will use the GitHub Checks API.

Which authentication type should you use?

- A. OpenID

B. GitHub App

C. a personal access token (PAT)

D. SAML

**Answer: B**

**Explanation:**

Write permission for the Checks API is only available to GitHub Apps.

Note: Authenticating as a GitHub App lets you do a couple of things:

- ⇒ You can retrieve high-level management information about your GitHub App.
- ⇒ You can request access tokens for an installation of the app.

Reference:

<https://docs.github.com/en/rest/guides/getting-started-with-the-checks-api>

**CertyIQ**

**Question: 296**

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:

1. Select the Triggers tab.
2. Enable Continuous integration.

Reference:

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

**CertyIQ**

**Question: 297**

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:

1. Select the Triggers tab.
2. Enable Continuous integration.

Reference:

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

**CertyIQ**

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:**

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

1. Select the Triggers tab.
2. Enable Continuous integration.

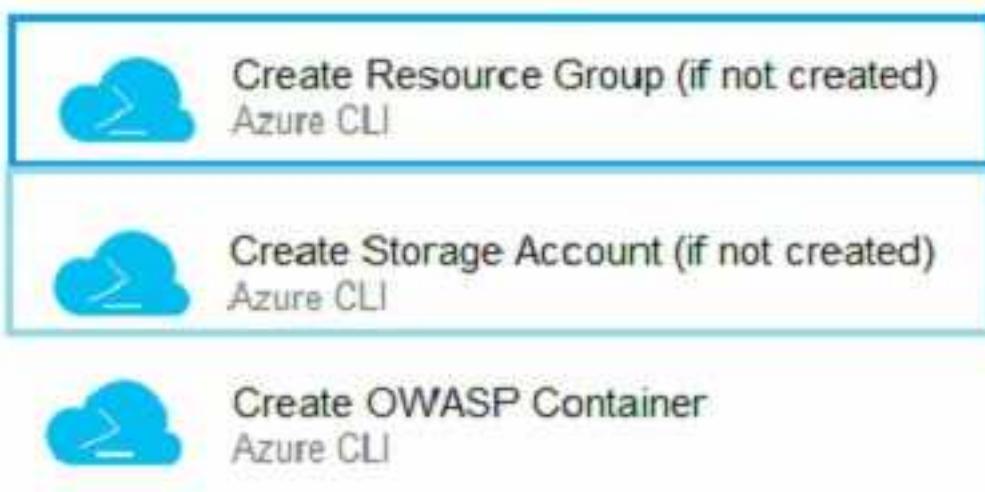
Reference:

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

**CertyIQ****Question: 299**

DRAG DROP -

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.

Select and Place:

| Tasks                   | Answer Area                                                                       |
|-------------------------|-----------------------------------------------------------------------------------|
| Convert Report Format   |                                                                                   |
| Build machine image     |                                                                                   |
| Publish Test Results    |  |
| Destroy OWASP Container |  |
| Call the Baseline Scan  |                                                                                   |
| Docker CLI installer    |                                                                                   |
| Download the file       |                                                                                   |

Answer:

| Tasks                   | Answer Area                                                                           |
|-------------------------|---------------------------------------------------------------------------------------|
| Convert Report Format   | Call the Baseline Scan                                                                |
| Build machine image     | Download the file                                                                     |
| Publish Test Results    |    |
| Destroy OWASP Container |    |
| Call the Baseline Scan  | Convert Report Format                                                                 |
| Docker CLI installer    |  |
| Download the file       |  |

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)

Azure CLI



Create Storage Account (if not created)

Azure CLI



Create OWASP Container

Azure CLI



Call the Baseline Scan

Azure CLI



Download the file

Azure CLI



Convert Report Format

PowerShell



Publish Test Results

Publish Test Results



Destroy OWASP Container

Azure CLI

Reference:

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

### Question: 300

CertyIQ

HOTSPOT -

You company uses a Git source-code repository.

You plan to implement GitFlow as a workflow strategy.

You need to identify which branch types are used for production code and preproduction code in the strategy.

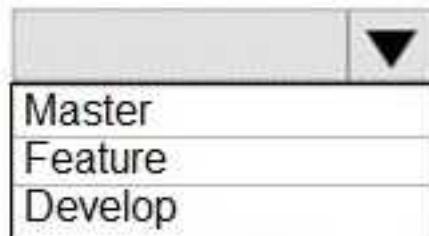
Which branch type should you identify for each code type? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

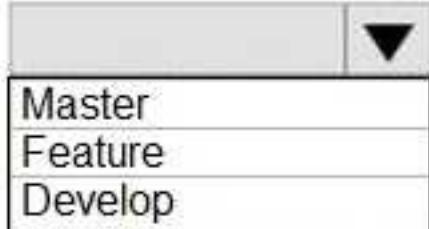
Hot Area:

## Answer Area

Production code:



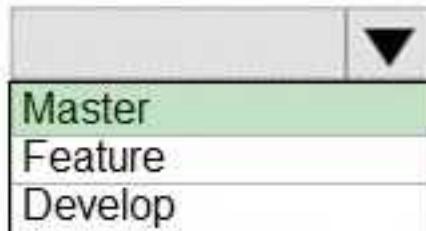
Preproduction code:



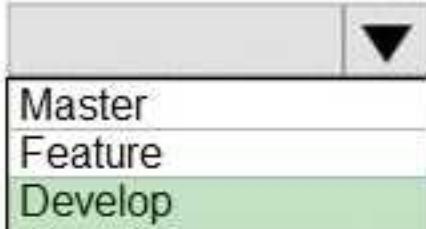
Answer:

## Answer Area

Production code:



Preproduction code:



### Explanation:

Box 1: Master -

The Master branch contains production code. All development code is merged into master in sometime.

Box 2: Develop -

The Develop branch contains pre-production code. When the features are finished then they are merged into develop.

Incorrect Answers:

During the development cycle, a variety of supporting branches are used:

- ⇒ Feature branches are used to develop new features for the upcoming releases. May branch off from develop and must merge into develop.

Reference:

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

**Question: 301**

CertyIQ

You have a build pipeline in Azure Pipelines that uses different jobs to compile an application for 10 different architectures.

The build pipeline takes approximately one day to complete.

You need to reduce the time it takes to execute the build pipeline.

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

NOTE: Each correct selection is worth one point.

- A. Move to a blue/green deployment pattern
- B. Create a deployment group
- C. Increase the number of parallel jobs
- D. Reduce the size of the repository
- E. Create an agent pool

**Answer: CE****Explanation:**

C. Increase the number of parallel jobs

E. Create an agent pool

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

**Question: 302**

CertyIQ

You are creating a build pipeline in Azure Pipelines.

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

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

What should you do?

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

**Answer: B****Explanation:**

A flaky test is a test that provides different outcomes, such as pass or fail, even when there are no changes in the source code or execution environment. Flaky tests also impact the quality of shipped code.

flaky test should be the answer

**Question: 303**

CertyIQ

DRAG DROP -

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.

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

Select and Place:

### Actions

Create an agent pool

Add the Puppet Agent extension to the virtual machines

Add and configure a deployment group job for the pipeline

Add the Azure Pipelines Agent extension to the virtual machines

Create a deployment group

Execute the pipeline

### Answer Area



### Answer:

#### Actions

Create an agent pool

Add the Puppet Agent extension to the virtual machines

Add and configure a deployment group job for the pipeline

Add the Azure Pipelines Agent extension to the virtual machines

Create a deployment group

Execute the pipeline

#### Answer Area

Create a deployment group

Add the Azure Pipelines Agent extension to the virtual machines

Add and configure a deployment group job for the pipeline

Execute the pipeline

### Explanation:

1- Create a deployment group

2- Add the Azure Pipelines Agent extension to the virtual machines

3- Add and configure a deployment group job for the pipeline

4- execute the pipeline

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 Triggers tab of the build pipeline, you select Enable continuous integration.

Does this meet the goal?

A. Yes

B. No

#### Answer: A

#### Explanation:

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

1. Select the Triggers tab.
2. Enable Continuous integration.

A continuous integration trigger on a build pipeline indicates that the system should automatically queue a new build whenever a code change is committed.

Reference:

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

#### Question: 305

CertyIQ

You have an Azure DevOps organization named Contoso and an Azure DevOps project named Project1.

You plan to use Microsoft-hosted agents to build container images that will host full Microsoft .NET Framework apps in a YAML pipeline in Project1.

What are two possible virtual machine images that you can use for the Microsoft-hosted agent pool? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. vs2017-win2016

B. ubuntu-16.04

C. win1803

D. macOS-10.13

E. vs.2015-win2012r2

#### Answer: AB

#### Explanation:

Windows that is supported - A

rest is obsolete

Ubuntu on which you can build image - B.

#### Question: 306

CertyIQ

HOTSPOT -

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.

Hot Area:

## Answer Area

JIRA:

Boards

Build pipelines

Release pipelines

Repos

Jenkins:

Boards

Build pipelines

Release pipelines

Repos

Octopus:

Boards

Build pipelines

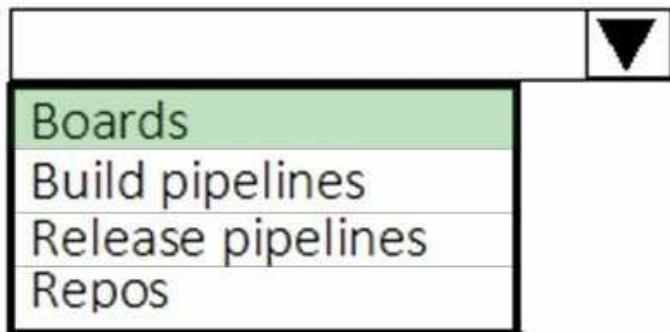
Release pipelines

Repos

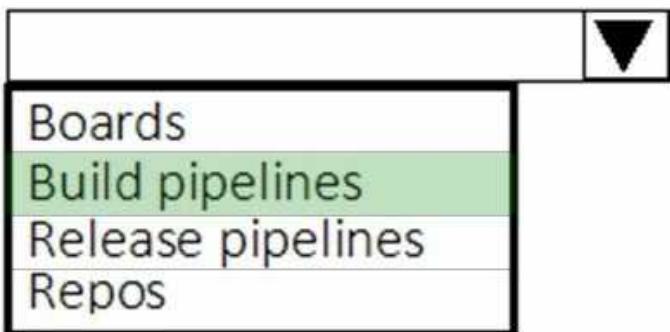
Answer:

## Answer Area

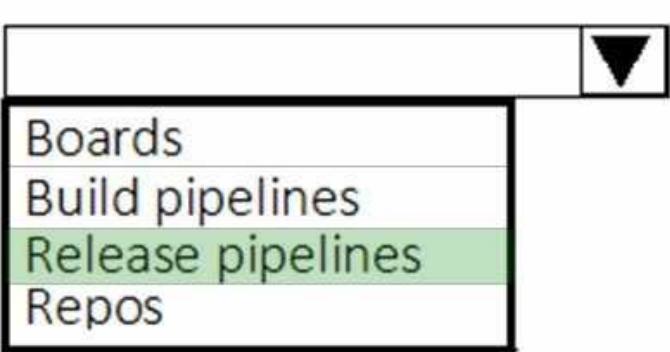
JIRA:



Jenkins:



Octopus:



### Explanation:

Reference:

<https://octopus.com/blog/octopus-jira-integration>

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

## Question: 307

CertyIQ

Your company has a project in Azure DevOps.

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

What should you use?

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

### Answer: B

### Explanation:

The options you can choose for a queuing policy are:

- ⇒ Number of parallel deployments
- ⇒ If you specify a maximum number of deployments, two more options appear:

- Deploy all in sequence
- Deploy latest and cancel the others: Use this option if you are producing releases faster than builds, and you only want to deploy the latest build.

Incorrect Answers:

C: Release 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.

Reference:

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

## Question: 308

CertyIQ

Your company develops a client banking application that processes a large volume of data. Code quality is an ongoing issue for the company. Recently, the code quality has deteriorated because of an increase in time pressure on the development team.

You need to implement static code analysis.

During which phase should you use static code analysis?

- A. integration testing
- B. staging
- C. production release
- D. build

Answer: D

Explanation:

Answer= Build -as static code analysis is done at compile time not runtime.

But developers don't intend to fix these issues due to sheer pressure, so it can be at the build time if you have good developers and can be at CI time when you want to enforce it, I think enforcing would be a better as developers will be obliged to fix them.

## Question: 309

CertyIQ

DRAG DROP -

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.

Select and Place:

**Actions****Answer Area**

Modify the configuration files to reference the Azure Artifacts feed.

Run an initial package restore.

Create a Microsoft Visual Studio project that includes all the packages.

Create an Azure Artifacts feed that uses upstream sources.

Create a NuGet package.

Create an npm package.

**Answer:****Actions****Answer Area**

Modify the configuration files to reference the Azure Artifacts feed.

Run an initial package restore.

Create a Microsoft Visual Studio project that includes all the packages.

Create an Azure Artifacts feed that uses upstream sources.

Create a NuGet package.

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.

**Explanation:****1. Create an azure artifacts feed that uses upstream sources**

Upstream sources enable you to use a single feed to store both the packages you produce and the packages you consume from both public packages managers (npmjs.com, NuGet.org, Maven Central, and PyPI) and Artifacts feeds.

**2. Modify the configuration files to reference the Arure Artifacts feed**

Since they were referencing the public feeds

**3. Run an initial package restore**

To pull the packages from the public feed and save them in the azure upstream feed:

Packages belonging to an upstream are available downstream soon after they are published, but will only show up in the feed's UI once they have been 'ingested,' which requires installing the package version for the first time in the downstream feed.

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

<https://docs.microsoft.com/en-us/azure/devops/artifacts/how-to/set-up-upstream-sources?view=azure-devops>

**Question: 310**

CertyIQ

**HOTSPOT -**

You have the Azure DevOps pipeline shown in the following exhibit.

The screenshot shows the Azure DevOps interface for a pipeline named 'PU Test'. On the left, there's a sidebar with icons for Overview, Boards, Repos, Pipelines, Environments, Releases, Library, Task groups, Deployment groups, Test Plans, and Artifacts. The 'Pipelines' icon is highlighted. The main area shows a pipeline named 'PartsUnlimitedE2E' with the following tasks:

- Get sources (Run on agent)
- Cloud Agent (Run on agent)
  - NuGet restore (NuGet Installer)
  - Compile Application (.NET Core)
  - Copy Files (Copy Files)
  - Publish Artifact (Publish Artifacts)

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.

Hot Area:

**Answer Area**

The pipeline has  job(s).

|   |
|---|
| 0 |
| 1 |
| 4 |

The pipeline has  task(s).

|   |
|---|
| 0 |
| 1 |
| 4 |

**Answer:**

## Answer Area

The pipeline has  job(s).

|   |
|---|
| 0 |
| 1 |
| 4 |

The pipeline has  task(s).

|   |
|---|
| 0 |
| 1 |
| 4 |

### Explanation:

Box 1: 1 -

The Cloud agent job only.

Box 2: 4 -

The pipeline has the four tasks: NuGet restore, Compile Application, Copy Files, and Publish Artifact.

Reference:

<https://azuredevopslabs.com/labs/azuredevops/continuousintegration/>

## Question: 311

CertyIQ

SIMULATION -

You have an Azure function hosted in an App Service plan named az400-123456789-func1.

You need to configure az400-123456789-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 explanation 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 configure az400-123456789-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.

Reference:

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

CertyIQ

**Question: 312**

DRAG DROP -

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

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

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

Select and Place:

**Actions**

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.

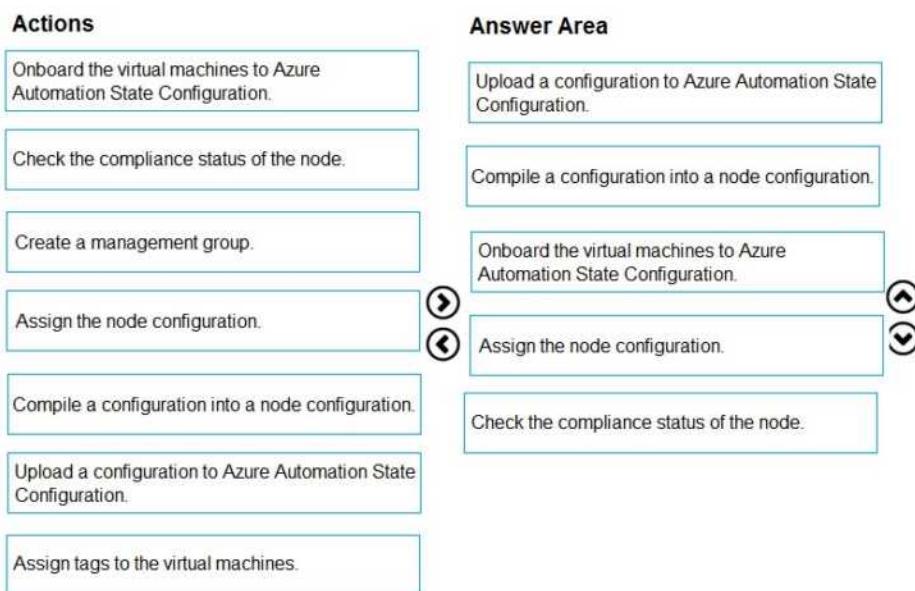
Upload a configuration to Azure Automation State Configuration.

Assign tags to the virtual machines.

**Answer Area**



**Answer:**



### Explanation:

1. Upload
2. Compile
3. Onboard
4. Assign the node configuration
5. Check

### Question: 313

CertyIQ

You are developing an application. The application source has multiple branches.

You make several changes to a branch used for experimentation.

You need to update the main branch to capture the changes made to the experimentation branch and override the history of the Git repository.

Which Git option should you use?

- A. Rebase
- B. Fetch
- C. Merge
- D. Push

### Answer: A

#### Explanation:

"Git rebase resequences the commit history of the target branch so that it contains all source branch commits, followed by all target branch commits since the last common commit. Another way to view it is that a rebase replays the changes in your target branch on top of the source branch history"

<https://docs.microsoft.com/en-us/azure/devops/repos/git/rebase?view=azure-devops&tabs=visual-studio-2019>

## Question: 314

CertyIQ

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 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:

"Pipeline caching can help reduce build time by allowing the outputs or downloaded dependencies from one run to be reused in later runs, thereby reducing or avoiding the cost to recreate or redownload the same files again. Caching is especially useful in scenarios where the same dependencies are downloaded over and over at the start of each run. This is often a time consuming process involving hundreds or thousands of network calls.

Caching can be effective at improving build time provided the time to restore and save the cache is less than the time to produce the output again from scratch. Because of this, caching may not be effective in all scenarios and may actually have a negative impact on build time."

Answer is No

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

## Question: 315

CertyIQ

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 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>

CertyIQ

### Question: 316

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 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>

CertyIQ

### Question: 317

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:

you can deploy several ARM templates in one deployment - just add different tasks or multiple ARM deployment steps in the task

CertyIQ

#### Question: 318

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.

Reference:

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

CertyIQ

#### Question: 319

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.

Reference:

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

CertyIQ

### Question: 320

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).

Reference:

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

CertyIQ

### Question: 321

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 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: B****Explanation:**

1. One of those outdated questions again <https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/utility/copy-and-publish-build-artifacts?view=azure-devops> "This task is deprecated. We recommend that you use Pipeline Artifacts." Answer is No in accordance to Microsoft recommendation
2. Very confusing! Here the deployment pipeline should download the artifacts and should not use copy and publish task as that should have been done in build pipeline already!

**CertyIQ****Question: 322**

You have a project in Azure DevOps named Project1. Project1 contains a pipeline that builds a container image named Image1 and pushes Image1 to an Azure container registry named ACR1. Image1 uses a base image stored in Docker Hub.

You need to ensure that Image1 is updated automatically whenever the base image is updated.  
What should you do?

- A. Enable the Azure Event Grid resource provider and subscribe to registry events.
- B. Add a Docker Hub service connection to Azure Pipelines.
- C. Create and run an Azure Container Registry task.**
- D. Create a service hook in Project1.

**Answer: C****Explanation:**

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

**Reference:**

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

**CertyIQ****Question: 323**

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>

CertyIQ

### Question: 324

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.

Reference:

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

CertyIQ

### Question: 325

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 resources in its respective group.

Does this meet the goal?

A. Yes

B. No

**Answer: A**

**Explanation:**

To deploy your solution, you can use either a single template or a main template with many related templates. The related template can be either a separate file that is linked to from the main template, or a template that is nested within the main template.

Reference:

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

**Question: 326**

CertyIQ

DRAG DROP -

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.

Select and Place:

**Azure Services**

**Answer Area**

Azure Artifacts

Source code:

Azure Pipelines

A common library used by multiple applications:

Azure Repos

Logs from automated tests and builds:

Azure Storage

Large and frequently updated binary assets:

Azure Test Plans

**Answer:**

## Azure Services

## Answer Area

|                  |                                                 |                 |
|------------------|-------------------------------------------------|-----------------|
| Azure Artifacts  | Source code:                                    | Azure Repos     |
| Azure Pipelines  | A common library used by multiple applications: | Azure Artifacts |
| Azure Repos      | Logs from automated tests and builds:           | Azure Pipelines |
| Azure Storage    | Large and frequently updated binary assets:     | Azure Storage   |
| Azure Test Plans |                                                 |                 |

### Explanation:

Box 1: Azure Repos -

Box 2: Azure Artifacts -

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

Box 3: Azure Pipelines -

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

Box 4: Azure Storage -

### Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/get-started/what-is-repos> <https://azure.microsoft.com/en-us/services/devops/artifacts/> <https://docs.microsoft.com/en-us/azure/devops/pipelines/test/review-continuous-test-results-after-build>

## Question: 327

CertyIQ

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

### Answer: B

### Explanation:

Upstream sources has nothing to do with having several versions of your package

## Question: 328

CertyIQ

You have a project in Azure DevOps named Project1. Project1 contains a build pipeline named Pipe1 that builds an

application named App1.

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. Add another self-hosted agent.
- B. Add a Docker Compose task to the build pipelines.
- C. Change the self-hosted agent to use Red Hat Enterprise Linux (RHEL) 8.
- D. Create two container jobs.**

**Answer: D**

**Explanation:**

To get more control over software dependencies and operating system, you can use Container jobs. Note that the decisions whether to run your pipeline inside a container and whether to use a self-hosted agent are independent. You can directly run your pipeline on a self-hosted agent, or inside a container. You can also execute your pipeline in a container on a Microsoft-hosted agent or on a self-hosted agent.

Incorrect Answers:

A: For additional control over hardware, you can use a self-hosted build agent.

Reference:

<http://thewindowsupdate.com/2019/09/09/resolving-complex-software-and-hardware-dependencies-in-azure-devops-pipelines/>

**Question: 329**

**CertyIQ**

SIMULATION -

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 explanation 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 'Content trust' settings for a container registry named 'myregistry'. The status is set to 'Enabled'. A note explains that enabling content trust allows pushing trusted images to the registry. The left sidebar lists services like Repositories, Webhooks, Replications, and Tasks, with 'Content trust' highlighted by a red box.

Reference:

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

### Question: 330

CertyIQ

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. adding users
- C. assigning entitlements
- D. procuring licenses

Answer: D

Explanation:

Incorrect Answers:

A: You can seamlessly replace existing solutions with group-based licensing to more easily manage licenses in Azure DevOps. You can use Group rules.

C: Member Entitlement Management APIs allow managing Entitlements that include -

- ⇒ License
- ⇒ Extensions
- ⇒ Project/Team memberships

Reference:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/migrate-to-group-based-resource-management?view=vsts&tabs=new-nav> <https://docs.microsoft.com/en-us/rest/api/azure/devops/memberentitlementmanagement/?view=azure-devops-rest-5.0>

**HOTSPOT -**

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 changed 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.

Hot Area:

**Answer Area**

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:

**Answer Area**

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:**

**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.

**CertyIQ**

**Question: 332**

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. CocoaPods
- D. Gradle

**Answer: D**

**Explanation:**

The Gradle build task now supports SonarQube analysis.

SonarQube analysis for Java.

In October 2016, we updated the Maven task to support SonarQube analysis (See [The Maven build task now simplifies SonarQube analysis](#)). This time, we are pleased to announce an updated Gradle task which makes it easy for Java developers using Gradle to trigger a SonarQube analysis in Visual Studio Team Services.

Using the Gradle task with SonarQube.

Just as for Maven, we have added a Code Analysis section in which you can now check the Run SonarQube Analysis checkbox, which then shows more options.

[+ Add build step...](#)

**gradlew build**

**Gradle**

**Copy Files to:** \$(build.artifactstagingdirectory) [Copy Files](#)

**Publish Artifact: drop**  
Publish Build Artifacts

**gradlew build**

Gradle Wrapper

gradlew

Options

Tasks

build

**JUnit Test Results**

Publish to TFS/Team Services



Test Results Files



Test Run Title

**Code Coverage**

Code Coverage Tool

None

**Advanced****Code Analysis**

Run SonarQube Analysis



SonarQube Endpoint

<https://sonarqube.com>[Manage](#)

SonarQube Project Name

MinecraftForge

SonarQube Project Key

MinecraftForge

SonarQube Project Version

2.0.2

The SonarQube server version is lower than 5.2.

**Control Options**

Enabled



Continue on error



Always run

**Reference:**<https://devblogs.microsoft.com/devops/the-gradle-build-task-now-supports-sonarqube-analysis/>**CertyIQ****Question: 333**

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. Maven
- B. CocoaPods
- C. Xcode
- D. Gulp

**Answer: A****Explanation:**

The SonarScanner for Maven is recommended as the default scanner for Maven projects.

The ability to execute the SonarQube analysis via a regular Maven goal makes it available anywhere Maven is available (developer build, CI server, etc.), without the need to manually download, setup, and maintain a SonarQube Runner installation. The Maven build already has much of the information needed for SonarQube to successfully analyze a project. By preconfiguring the analysis based on that information, the need for manual configuration is reduced significantly.

**Reference:**

**Question: 334**

You have an Azure subscription named Subscription1 that contains a custom Azure policy named Policy1. Policy1 is an audit policy that monitors naming convention compliance for the resources deployed to Subscription1. You have a pipeline named Pipeline1 in Azure Pipelines. Pipeline1 deploys Azure Resource Manager (ARM) resources to Subscription1.

You need to ensure that the resources deployed by Pipeline1 comply with Policy1.

What should you add to Pipeline1?

- A. a pre-deployment task that runs a security and compliance assessment
- B. a post-deployment task that runs a security and compliance assessment
- C. an ARM template deployment task to assign Policy1 to Subscription1
- D. an ARM template deployment task to deploy Policy1 to Subscription1

**Answer: A**

**Explanation:**

Check policy compliance with gates.

Prepare -

1. Create an Azure Policy in the Azure portal. There are several predefined sample policies that can be applied to a management group, subscription, and resource group.
2. In Azure DevOps create a release pipeline that contains at least one stage, or open an existing release pipeline.
3. Add a pre- or post-deployment condition that includes the Security and compliance assessment task as a gate.

## Post-deployment configuration

Stage 2

### Post-deployment approvals

Select the users who can approve or decline this deployment.

### Gates ▾

Define gates to evaluate after the deployment stage.

The delay before evaluation

5

Deployment gates ⓘ

#### Code Coverage

Get code coverage data for a build

#### Invoke Azure Function

Invoke an Azure Function as a part of your pipeline.

#### Invoke REST API

Invoke a REST API as a part of your pipeline.

#### Query Classic Azure Monitor Alerts

Observe the configured classic Azure monitor rules for active alerts.

#### Query Work Items

Executes a work item query and checks for the number of items returned.

#### Security and compliance assessment

Security and compliance assessment with Azure policies on resources that belong to the resource group and Azure subscription

+ Add ▾

## Post-deployment configuration

Stage 2

### Post-deployment approvals

Select the users who can approve or decline this deployment.

### Gates ▾

Define gates to evaluate after the deployment stage.

The delay before evaluation

5

Deployment gates ⓘ

+ Add ▾

#### Code Coverage

Get code coverage data for a build

#### Invoke Azure Function

Invoke an Azure Function as a part of your pipeline.

#### Invoke REST API

Invoke a REST API as a part of your pipeline.

#### Query Classic Azure Monitor Alerts

Observe the configured classic Azure monitor rules for active alerts.

#### Query Work Items

Executes a work item query and checks for the number of items returned.

#### Security and compliance assessment

Security and compliance assessment with Azure policies on resources that belong to the resource group and Azure subscription

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/policies/azure-policy>

Comments

### Question: 335

CertyIQ

HOTSPOT -

You plan to use Desired State Configuration (DSC) to maintain the configuration state of virtual machines that run Windows Server.

You need to perform the following:

- ⇒ Install Internet Information Services (IIS) on the virtual machines.
- ⇒ Update the default home page of the IIS web server.

How should you configure the DSC configuration file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

```
Configuration WebServerConfig {
 Import-DscResource -ModuleName PsDesiredStateConfiguration
 Node 'localhost' {

| |
|------------------------|
| Service |
| WindowsFeature |
| WindowsOptionalFeature |
| WindowsProcess |

 WebServer {
 Ensure = "Present"
 Name = "Web-Server"
 }

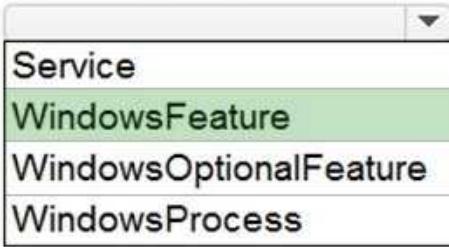
 DefaultHomePage {

| |
|---------|
| Archive |
| File |
| Package |
| Script |

 Ensure = 'Present'
 SourcePath = '\\server1
\DS/Resources\web\index.htm'
 DestinationPath = 'c:\inetpub\wwwroot'
 }
 }
}
```

Answer:

## Answer Area

```
Configuration WebServerConfig {
 Import-DscResource -ModuleName PsDesiredStateConfiguration
 Node 'localhost' {
 
 WebServer {
 Ensure = "Present"
 Name = "Web-Server"
 }

 
 DefaultHomePage {
 Ensure = 'Present'
 SourcePath = '\\\\server1\\DSCResources\\web\\index.htm'
 DestinationPath = 'c:\\inetpub\\wwwroot'
 }
 }
}
```

### Explanation:

Box 1: WindowsFeature -

Example:

Configuration WebsiteTest

# Import the module that contains the resources we're using.

```
Import-DscResource -ModuleName PsDesiredStateConfiguration
```

# The Node statement specifies which targets this configuration will be applied to.

Node 'localhost'

# The first resource block ensures that the Web-Server (IIS) feature is enabled.

WindowsFeature WebServer

Ensure = "Present"

Name = "Web-Server"

Box 2: File -

Example continued:

# The second resource block ensures that the website content copied to the website root folder.

File WebsiteContent

Ensure = 'Present'

SourcePath = 'c:\\test\\index.htm'

DestinationPath = 'c:\inetpub\wwwroot'

Reference:

<https://docs.microsoft.com/en-us/powershell/scripting/dsc/quickstarts/website-quickstart>

### Question: 336

CertyIQ

You have a project in Azure DevOps.

You need to push notifications about pull requests to a Microsoft Teams channel. The solution must minimize development effort.

What should you do?

- A. Install the Azure Pipelines app for Teams and configure a subscription to receive notifications in the channel.
- B. Use Azure Automation to connect to the Azure DevOps REST API and send messages to Teams.
- C. Install the Azure Repos app for Teams and configure a subscription to receive notifications in the channel.**
- D. Use an Azure function to connect to the Azure DevOps REST API and send messages to Teams.

### Answer: C

#### Explanation:

If you use Microsoft Teams, you can use the Azure Repos app for Teams to easily monitor your repositories.

Set up and manage subscriptions to receive notifications in your channel whenever code is pushed/checked in or when a pull request (PR) is created, updated or merged. The app supports monitoring both Git and Team Foundation Version Control (TFVC) repositories.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/integrations/repos-teams>

### Question: 337

CertyIQ

HOTSPOT -

You are creating a YAML-based Azure pipeline to deploy an Azure Data Factory instance that has the following requirements:

- ⇒ If a Data Factory instance exists already, the instance must be overwritten.
- ⇒ No other resources in a resource group named Fabrikam must be affected.

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

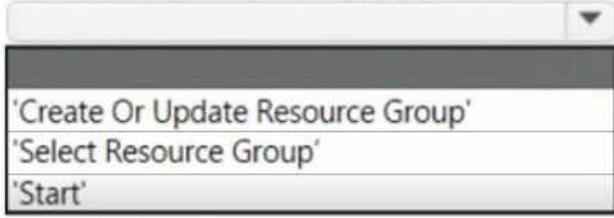
NOTE: Each correct selection is worth one point.

Hot Area:

```
steps:
- task: AzureResourceManagerTemplateDeployment@3

inputs:
 deploymentScope: 'Resource Group'

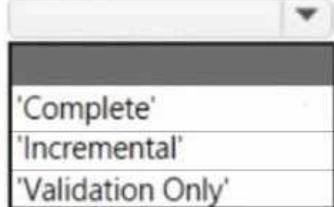
 azureResourceManagerConnection: 'Fabrikam Corporate(a41fb3ed-a2aa-42f0-a7ac-8fcc6ef0c5db)'
 subscriptionId: 'a41de0ed-a2aa-42f0-a7ac-8fcc6ef0c5db'

 action: 
 'Create Or Update Resource Group'
 'Select Resource Group'
 'Start'

 resourceGroupName: 'Fabrikam'

 location: 'West US'

 templateLocation: 'Linked artifact'

 deploymentMode: 
 'Complete'
 'Incremental'
 'Validation Only'
```

### Answer:

```
steps:
- task: AzureResourceManagerTemplateDeployment@3

inputs:
 deploymentScope: 'Resource Group'

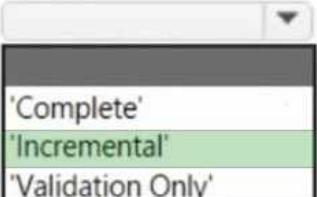
 azureResourceManagerConnection: 'Fabrikam Corporate(a41fb3ed-a2aa-42f0-a7ac-8fcc6ef0c5db)'
 subscriptionId: 'a41de0ed-a2aa-42f0-a7ac-8fcc6ef0c5db'

 action: 
 'Create Or Update Resource Group'
 'Select Resource Group'
 'Start'

 resourceGroupName: 'Fabrikam'

 location: 'West US'

 templateLocation: 'Linked artifact'

 deploymentMode: 
 'Complete'
 'Incremental'
 'Validation Only'
```

**Question: 338**

CertyIQ

You have an Azure DevOps project that produces Node Package Manager (npm) packages. Multiple projects consume the packages.

You need to configure Azure Artifacts to ensure that both the latest and pre-release versions of the packages are available for consumption.

What should you do?

- A. Create two feed views named @prerelease and @release. Set @release as the default view. Configure a release pipeline that tags the packages as release after successful testing.
- B. Create a feed view named @prerelease. Configure a release pipeline that tags the packages as release after successful testing.
- C. Create two feed views named @prerelease and @default. Configure a release pipeline that promotes a package to the @default view after successful testing.
- D. Create two feed views named @prerelease and @release. Set @release as the default view. Configure a release pipeline that promotes a package to the @release view after successful testing.

**Answer: D****Explanation:**

When a package is ready for early adopters, select that package from within your feed and promote it to the @prerelease view. When the package is deemed of sufficient quality to be released, promote that package to the @release view.

Reference:

<https://learn.microsoft.com/en-us/azure/devops/artifacts/concepts/best-practices?view=azure-devops#create-and-publish-packages>

**Question: 339**

CertyIQ

You have an Azure subscription that contains the resources shown in the following table.

| Name     | Type                    |
|----------|-------------------------|
| Feed1    | Azure Artifacts feed    |
| Project1 | Project in Azure DevOps |

Project produces npm packages that are published to Feed1. Feed1 is consumed by multiple projects. You need to ensure that only tested packages are available for consumption. The solution must minimize development effort.

What should you do?

- A. Create a feed view named @release and set @release as the default view. After the npm packages test successfully, configure a release pipeline that promotes a package to the @release view.
- B. Create a feed view named @release and set @release as the default view. After the npm packages test successfully, configure a release pipeline that tags the packages as release.
- C. Create a feed view named @default. After the npm packages test successfully, configure a release pipeline that tags the packages as release.
- D. Create a feed view named @default. After the npm packages test successfully, configure a release pipeline that promotes a package to the @default view.

**Answer: A**

CertyIQ

**Question: 340**

Your company has an Azure DevOps project that produces Node Package Manager (npm) packages. Multiple projects consume the packages.

You need to minimize the amount of disk space used by older packages in Azure Artifacts.

What should you modify?

- A. the retention settings of the project's release
- B. the retention settings of the project's pipeline**
- C. the retention settings of the project's tests
- D. the retention settings of the company pipeline

**Answer: B**

**Explanation:**

<https://learn.microsoft.com/en-us/azure/devops/pipelines/policies/retention?view=azure-devops&tabs=yaml>

**Question: 341**

CertyIQ

DRAG DROP

You have an Azure DevOps pipeline that is used to deploy a Node.js app.

You need to ensure that the dependencies are cached between builds.

How should you configure the deployment YAML? To answer, drag the appropriate values to the correct targets. 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**

|                                      |
|--------------------------------------|
| always()                             |
| build.sh                             |
| eq(variables.CACHE_RESTORED, 'true') |
| integrationtest.sh                   |
| ne(variables.CACHE_RESTORED, 'true') |
| npm install                          |

```
...
variables:
 npm_config_cache: $(Pipeline.Workspace)/.npm
steps:
- task: Cache@2
 inputs:
 key: 'npm | $(Agent.OS) | package-lock.json'
 restoreKeys:
 - npm | $(Agent.OS)
 path: $(npm_config_cache)
 cacheHitVar: CACHE_RESTORED

- script: $(IntegrationTestScript)
 condition: $(IntegrationTestCondition)
 ...

```

**Answer:**

## Answer Area

```
...
variables:
 npm_config_cache: $(Pipeline.Workspace)/.npm

steps:
- task: Cache@2
 inputs:
 key: 'npm | $(Agent.OS) | package-lock.json'
 restoreKeys: |
 npm | $(Agent.OS)
 path: $(npm_config_cache)
 cacheHitVar: CACHE_RESTORED

- script: build.sh
 condition: ne(variables.CACHE_RESTORED, 'true')
...
```

CertyIQ

## Question: 342

HOTSPOT -

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.

Hot Area:

## Answer Area

git gc

- aggressive
- auto
- force
- no-prune

git --expire now

- merge
- prune
- rebase
- reset

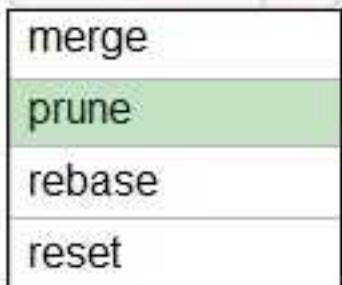
Answer:

## Answer Area

git gc



git --expire now



### Explanation:

Box 1: --aggressive -

Cleanup unnecessary files and optimize the local repository:

git gc --aggressive

Box 2: prune -

Prune all unreachable objects from the object database:

git prune

Reference:

<https://gist.github.com/Zoramite/2039636>

## Question: 343

CertyIQ

SIMULATION -

You plan to deploy a template named D:\Deploy.json to a resource group named Deploy-lod123456789.

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 explanation below.

### Explanation:

1. Sign in to the portal.
2. Choose template Deploy-lod123456789
3. Select Edit template, and then paste your JSON template code into the code window.
4. Change the ASddressPrefixes to 10.0.0.0/24 in order to support only 256 total IP addresses.  
addressSpace": "addressPrefixes": ["10.0.0.0/24"],

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

"subnets": [

    "name": "firstSubnet",

    "properties":

        "addressPrefix": "10.0.0.0/24"

6. Select Save.

# 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  Create new  Use existing

Resource group location

local

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.

# Microsoft Azure Stack - Administration

+ Create a resource

All services

★ FAVORITES

Dashboard

All resources

Resource groups

Virtual machines

Recent

Plans

Offers

Monitor

Marketplace management

Home > New > Custom deployment

## Custom deployment

Deploy from a custom template

Template

Edit template

Parameters

Edit parameters

Subscription

Default Provider Subscription

Resource group

Create new  Use existing

test-rg

Resource group location

US West

Create

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

Reference:

<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>

## Question: 344

CertyIQ

SIMULATION -

You need to configure an Azure web app named az400-123456789-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 explanation below.

Explanation:

1. In the Azure portal, navigate to the az400-123456789-main app's management page. In the app's left menu, click Configuration > Application settings.

The screenshot shows the Azure portal configuration interface for the 'my-core-app' app service. The left sidebar lists various configuration options like Security, Deployment, Quickstart, etc., with 'Configuration' selected. The main pane shows the 'Application settings' tab highlighted. A table lists the environmental variable 'MAX\_ITEMS' with the value '50'. Below it, the 'Connection strings' section is shown but contains no entries.

| Name      | Value | Type | deployment... |
|-----------|-------|------|---------------|
| MAX_ITEMS | 50    |      |               |

2. Click New Application settings

3. Enter the following:

- ⇒ Name: MAX\_ITEMS
- ⇒ Value: 50

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/configure-common>

## Question: 345

CertyIQ

DRAG DROP -

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.  
Select and Place:

## Commands

## Answer Area

helm install

kubectl create

helm completion

helm init

helm serve



Answer:

## Commands

## Answer Area

helm install

kubectl create

kubectl create

helm init

helm completion

helm install



helm init

helm serve

## Explanation:

Step 1: Kubectl create -

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

Example: Service account with cluster-admin role

```
$ kubectl create -f rbac-config.yaml
```

```
serviceaccount "tiller" created
```

```
clusterrolebinding "tiller" created
```

```
$ helm init --service-account tiller
```

Step 2: helm init -

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

Step 3: helm install -

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

Reference:

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

[https://docs.helm.sh/using\\_helm/#tiller-namespaces-and-rbac](https://docs.helm.sh/using_helm/#tiller-namespaces-and-rbac)

CertyIQ

## Question: 346

Your company builds a multi-tier web application.

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

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

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

- ⇒ Minimizes the cost of Azure hosting
- ⇒ Provisions the virtual machines automatically
- ⇒ Uses the custom Azure Resource Manager template to provision the virtual machines

What should you do?

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

B. In Azure DevOps, configure new tasks in the release pipeline to deploy to Azure Cloud Services.

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

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

## Answer: D

### Explanation:

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

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

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

Reference:

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

DRAG DROP -

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.

Select and Place:

## Answer Area

Private

Public

Shared

Group1:

Group2:

Group3:

Answer:

## Answer Area

Private

Public

Shared

Group1:

Private

Group2:

Public

Group3:

Shared

### Explanation:

Box1: Private -

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

#### Box 2: Public -

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

#### Box 3: Shared -

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

#### Reference:

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

CertyIQ

### Question: 348

#### SIMULATION -

You need to ensure that the https://contoso.com/statushook webhook is called every time a repository named az400123456789acr1 receives a new version of an image named dotnetapp.

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

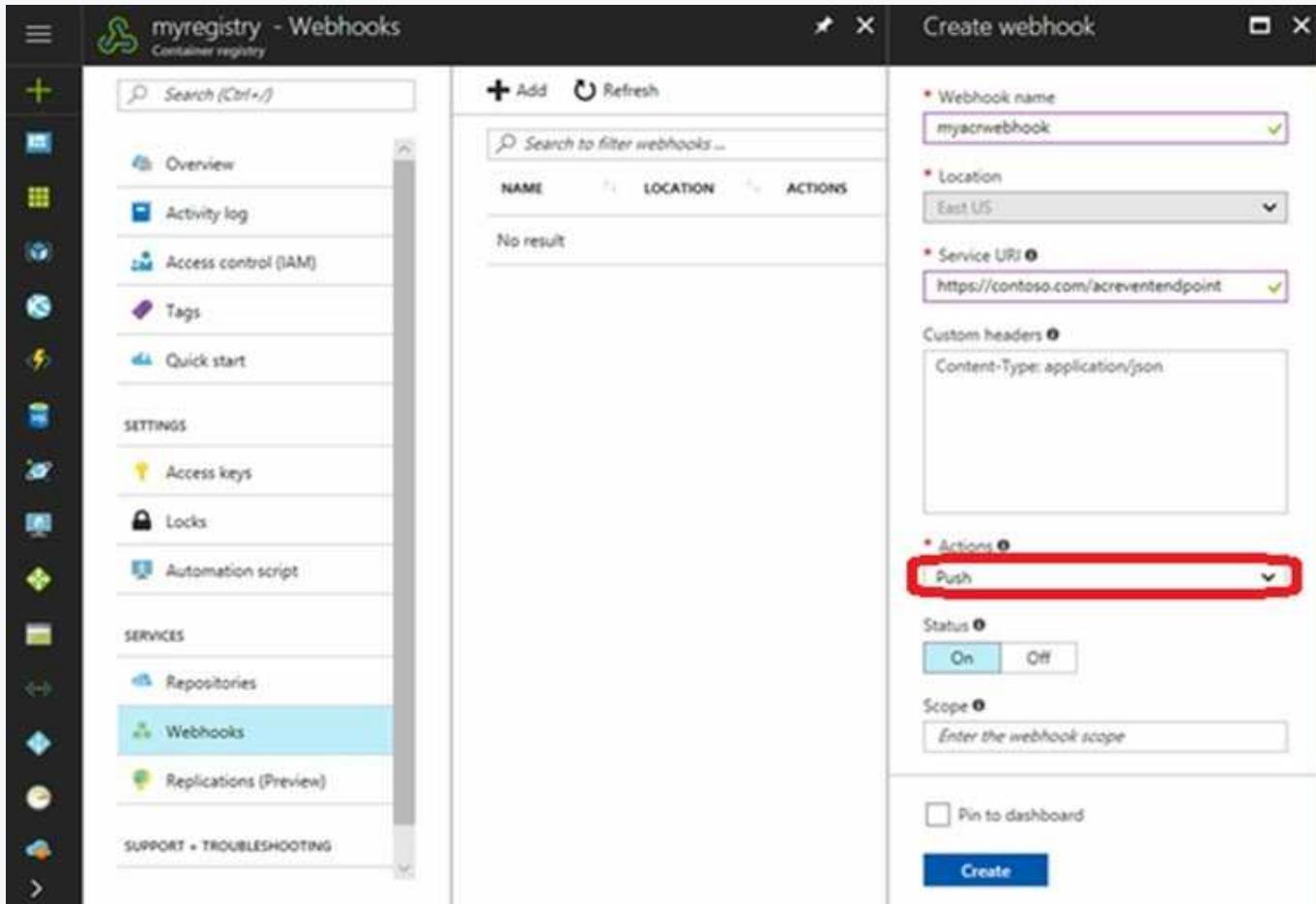
#### Answer:

See explanation below.

#### Explanation:

1. Sign in to the Azure portal.
2. Navigate to the container registry az400123456789acr1.
3. Under Services, select Webhooks.
4. Select the existing webhook https://contoso.com/statushook, and double-click on it to get its properties.
5. For Trigger actions select image push

Example web hook:



#### Reference:

**Question: 349**

HOTSPOT -

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

| Deployment   | Requirement                                                              |
|--------------|--------------------------------------------------------------------------|
| Deployment 1 | Use files stored on an SMB-based share from the container's file system. |
| Deployment 2 | Use files stored 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.

Hot Area:

**Answer Area**

Deployment 1:

driver: secrets-store.csi.k8s.io  
blobfuse-flexvol  
provisioner: kubernetes.io/azure-disk  
provisioner: kubernetes.io/azure-file  
volume.beta.kubernetes.io/storage-provisioner

Deployment 2:

driver: secrets-store.csi.k8s.io  
blobfuse-flexvol  
provisioner: kubernetes.io/azure-disk  
provisioner: kubernetes.io/azure-file  
volume.beta.kubernetes.io/storage-provisioner

Deployment 3:

driver: secrets-store.csi.k8s.io  
blobfuse-flexvol  
provisioner: kubernetes.io/azure-disk  
provisioner: kubernetes.io/azure-file  
volume.beta.kubernetes.io/storage-provisioner

**Answer:**

## Answer Area

### Deployment 1:

```
driver: secrets-store.csi.k8s.io
blobfuse-flexvol
provisioner: kubernetes.io/azure-disk
provisioner: kubernetes.io/azure-file
volume.beta.kubernetes.io/storage-provisioner
```

### Deployment 2:

```
driver: secrets-store.csi.k8s.io
blobfuse-flexvol
provisioner: kubernetes.io/azure-disk
provisioner: kubernetes.io/azure-file
volume.beta.kubernetes.io/storage-provisioner
```

### Deployment 3:

```
driver: secrets-store.csi.k8s.io
blobfuse-flexvol
provisioner: kubernetes.io/azure-disk
provisioner: kubernetes.io/azure-file
volume.beta.kubernetes.io/storage-provisioner
```

#### Explanation:

Deployment 1: provisioner: kubernetes.io/azure-file

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

Deployment 2: provisioner: kubernetes.io/azure-disk

Deployment 3: driver: secrets-store.csi.k8s.io

Azure Key vault provider for Secrets Store CSI driver allows you to access secrets stored in an Azure Key vault instance. The Secrets Store CSI driver secrets-store.csi.k8s.io allows the cluster to mount secrets stored in Azure Key vault into the pods as a volume.

Incorrect Answers:

blobfuse-flexvolume: This driver allows Kubernetes to access virtual filesystem backed by the Azure Blob storage.

Note: azurekeyvault-flexvolume has been deprecated and replaced by the Azure Key Vault Provider for Secret Store CSI Driver.

Reference:

<https://docs.microsoft.com/en-us/bs-cyrl-ba/azure/aks/azure-files-dynamic-pv> <https://docs.microsoft.com/en-us/az-ure/aks/azure-disks-dynamic-pv> [https://docs.microsoft.com/en-us/samples/azure-samples/secrets-store-csi-with-aks-akv/](https://docs.microsoft.com/en-us/samples/azure-samples/secrets-store-csi-with-aks-akv/secrets-store-csi-with-aks-akv/)

## Question: 350

CertyIQ

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

### Answer: C

#### Explanation:

Cherry-pick a pull request -

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

1. In a completed pull request, select Cherry-pick, or for an active pull request, select Cherry-pick from the ... menu. Cherry-picking a pull request in this way creates a new branch with the copied changes. Merge into a target branch in a second pull request.
2. In Target branch, enter the branch you want to merge the copied changes.
3. In Topic branch name, enter a new branch to contain the copied changes, then select Cherry-pick.
4. Select Create pull request to merge the topic branch into the target branch to complete the cherry-pick.

Reference:

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

CertyIQ

### Question: 351

DRAG DROP -

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.

Select and Place:

#### Actions

#### Answer Area

Delete and recreate the repository.

Run the `git reflog expire` command.

Run the `git add .gitignore` command.

Add Config.json to the `.gitignore` file.

Run the `git commit` command.



#### Answer:

**Actions**

Delete and recreate the repository.

Run the git reflog expire command.

Run the git add .gitignore command.

Add Config.json to the .gitignore file.

Run the git commit command.

**Answer Area**

Add Config.json to the .gitignore file.

Run the git add .gitignore command.

Run the git commit command.

**Explanation:**

Add Config.json to the .gitignore file.

Run the git add .gitignore command.

Run the git commit command.

**Question: 352****CertyIQ**

You are designing a build pipeline in Azure Pipelines.

The pipeline requires a self-hosted agent. The build pipeline will run once daily and will take 30 minutes to complete.

You need to recommend a compute type for the agent. The solution must minimize costs.

What should you recommend?

- A. an Azure Kubernetes Service (AKS) cluster
- B. Azure Container Instances
- C. an Azure virtual machine scale set**
- D. Azure virtual machines

**Answer: C****Explanation:**

It requires self-hosted agent rather than Microsoft-hosted agent. It is better to use scale set according to the following link <https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops&tabs=browser>. Azure virtual machine scale set agents are a form of self-hosted agents that can be auto-scaled to meet your demands. This elasticity reduces your need to run dedicated agents all the time. Unlike Microsoft-hosted agents, you have flexibility over the size and the image of machines on which agents run. You specify a virtual machine scale set, a number of agents to keep on standby, a maximum number of virtual machines in the scale set, and Azure Pipelines manages the scaling of your agents for you. For more information, see Azure virtual machine scale set agents.

**HOTSPOT -**

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.

Hot Area:

**Answer Area**

|                                                                                                                                                                                                                                                             |                          |      |                          |        |                          |      |                          |     |                          |                                                                                                                                                                                                                                                     |    |                          |    |                          |    |                          |    |                          |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|------|--------------------------|--------|--------------------------|------|--------------------------|-----|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|--------------------------|----|--------------------------|----|--------------------------|----|--------------------------|--|
| git                                                                                                                                                                                                                                                         | <input type="checkbox"/> | v3.0 | "Release v3.0"           |        |                          |      |                          |     |                          |                                                                                                                                                                                                                                                     |    |                          |    |                          |    |                          |    |                          |  |
| <table border="1"> <tr><td>add</td><td><input type="checkbox"/></td></tr> <tr><td>commit</td><td><input type="checkbox"/></td></tr> <tr><td>push</td><td><input type="checkbox"/></td></tr> <tr><td>tag</td><td><input type="checkbox"/></td></tr> </table> |                          | add  | <input type="checkbox"/> | commit | <input type="checkbox"/> | push | <input type="checkbox"/> | tag | <input type="checkbox"/> | <table border="1"> <tr><td>-a</td><td><input type="checkbox"/></td></tr> <tr><td>-b</td><td><input type="checkbox"/></td></tr> <tr><td>-c</td><td><input type="checkbox"/></td></tr> <tr><td>-m</td><td><input type="checkbox"/></td></tr> </table> | -a | <input type="checkbox"/> | -b | <input type="checkbox"/> | -c | <input type="checkbox"/> | -m | <input type="checkbox"/> |  |
| add                                                                                                                                                                                                                                                         | <input type="checkbox"/> |      |                          |        |                          |      |                          |     |                          |                                                                                                                                                                                                                                                     |    |                          |    |                          |    |                          |    |                          |  |
| commit                                                                                                                                                                                                                                                      | <input type="checkbox"/> |      |                          |        |                          |      |                          |     |                          |                                                                                                                                                                                                                                                     |    |                          |    |                          |    |                          |    |                          |  |
| push                                                                                                                                                                                                                                                        | <input type="checkbox"/> |      |                          |        |                          |      |                          |     |                          |                                                                                                                                                                                                                                                     |    |                          |    |                          |    |                          |    |                          |  |
| tag                                                                                                                                                                                                                                                         | <input type="checkbox"/> |      |                          |        |                          |      |                          |     |                          |                                                                                                                                                                                                                                                     |    |                          |    |                          |    |                          |    |                          |  |
| -a                                                                                                                                                                                                                                                          | <input type="checkbox"/> |      |                          |        |                          |      |                          |     |                          |                                                                                                                                                                                                                                                     |    |                          |    |                          |    |                          |    |                          |  |
| -b                                                                                                                                                                                                                                                          | <input type="checkbox"/> |      |                          |        |                          |      |                          |     |                          |                                                                                                                                                                                                                                                     |    |                          |    |                          |    |                          |    |                          |  |
| -c                                                                                                                                                                                                                                                          | <input type="checkbox"/> |      |                          |        |                          |      |                          |     |                          |                                                                                                                                                                                                                                                     |    |                          |    |                          |    |                          |    |                          |  |
| -m                                                                                                                                                                                                                                                          | <input type="checkbox"/> |      |                          |        |                          |      |                          |     |                          |                                                                                                                                                                                                                                                     |    |                          |    |                          |    |                          |    |                          |  |

Answer:

**Answer Area**

|                                                                                                                                                                                                                                                                        |                                     |      |                          |        |                          |      |                          |     |                                     |                                                                                                                                                                                                                                                                           |    |                                     |    |                          |    |                          |    |                                     |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|------|--------------------------|--------|--------------------------|------|--------------------------|-----|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|-------------------------------------|----|--------------------------|----|--------------------------|----|-------------------------------------|--|
| git                                                                                                                                                                                                                                                                    | <input type="checkbox"/>            | v3.0 | "Release v3.0"           |        |                          |      |                          |     |                                     |                                                                                                                                                                                                                                                                           |    |                                     |    |                          |    |                          |    |                                     |  |
| <table border="1"> <tr><td>add</td><td><input type="checkbox"/></td></tr> <tr><td>commit</td><td><input type="checkbox"/></td></tr> <tr><td>push</td><td><input type="checkbox"/></td></tr> <tr><td>tag</td><td><input checked="" type="checkbox"/></td></tr> </table> |                                     | add  | <input type="checkbox"/> | commit | <input type="checkbox"/> | push | <input type="checkbox"/> | tag | <input checked="" type="checkbox"/> | <table border="1"> <tr><td>-a</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>-b</td><td><input type="checkbox"/></td></tr> <tr><td>-c</td><td><input type="checkbox"/></td></tr> <tr><td>-m</td><td><input checked="" type="checkbox"/></td></tr> </table> | -a | <input checked="" type="checkbox"/> | -b | <input type="checkbox"/> | -c | <input type="checkbox"/> | -m | <input checked="" type="checkbox"/> |  |
| add                                                                                                                                                                                                                                                                    | <input type="checkbox"/>            |      |                          |        |                          |      |                          |     |                                     |                                                                                                                                                                                                                                                                           |    |                                     |    |                          |    |                          |    |                                     |  |
| commit                                                                                                                                                                                                                                                                 | <input type="checkbox"/>            |      |                          |        |                          |      |                          |     |                                     |                                                                                                                                                                                                                                                                           |    |                                     |    |                          |    |                          |    |                                     |  |
| push                                                                                                                                                                                                                                                                   | <input type="checkbox"/>            |      |                          |        |                          |      |                          |     |                                     |                                                                                                                                                                                                                                                                           |    |                                     |    |                          |    |                          |    |                                     |  |
| tag                                                                                                                                                                                                                                                                    | <input checked="" type="checkbox"/> |      |                          |        |                          |      |                          |     |                                     |                                                                                                                                                                                                                                                                           |    |                                     |    |                          |    |                          |    |                                     |  |
| -a                                                                                                                                                                                                                                                                     | <input checked="" type="checkbox"/> |      |                          |        |                          |      |                          |     |                                     |                                                                                                                                                                                                                                                                           |    |                                     |    |                          |    |                          |    |                                     |  |
| -b                                                                                                                                                                                                                                                                     | <input type="checkbox"/>            |      |                          |        |                          |      |                          |     |                                     |                                                                                                                                                                                                                                                                           |    |                                     |    |                          |    |                          |    |                                     |  |
| -c                                                                                                                                                                                                                                                                     | <input type="checkbox"/>            |      |                          |        |                          |      |                          |     |                                     |                                                                                                                                                                                                                                                                           |    |                                     |    |                          |    |                          |    |                                     |  |
| -m                                                                                                                                                                                                                                                                     | <input checked="" type="checkbox"/> |      |                          |        |                          |      |                          |     |                                     |                                                                                                                                                                                                                                                                           |    |                                     |    |                          |    |                          |    |                                     |  |

**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>

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.

Reference:

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

**Question: 355**

**CertyIQ**

DRAG DROP -

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.

Select and Place:

**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: an Azure Key Vault access policy

RBAC

**Explanation:**

Delete key vault - RBAC

Access to secrets - Vault Policy

<https://docs.microsoft.com/en-us/azure/key-vault/general/security-overview>**Question: 356****CertyIQ**

DRAG DROP -

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.

Select and Place:

**Actions****Answer Area**

Set the template parameters.

Create a package.

Create a release pipeline.



Create a job agent.

Add an Azure Resource Group Deployment task.

**Answer:**

**Actions****Answer Area**

Set the template parameters.

Create a release pipeline.

Create a package.

Add an Azure Resource Group Deployment task.

Create a release pipeline.

Set the template parameters.

Create a job agent.

Add an Azure Resource Group Deployment task.

**Explanation:**

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>

**CertyIQ****Question: 357**

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: A****Explanation:**

Modify the integrations options' since the Report deployment status to the repository its inside integration options

**CertyIQ****Question: 358**

SIMULATION -

You plan to add a new web farm that will be published by using an IP address of 10.0.0.5.

You need to allow traffic from the web farm to an Azure Database for MySQL server named az400-123456789-mysql.

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

## Answer:

See explanation below.

### Explanation:

Server-level firewall rules can be used to manage access to an Azure Database for MySQL Server from a specified IP address or a range of IP addresses.

Create a server-level firewall rule in the Azure portal

1. On the MySQL server page, under Settings heading, click Connection Security to open the Connection Security page for the Azure Database for MySQL.

The screenshot shows the 'mydemoserver - Connection security' page in the Azure portal. The left sidebar has a red box around the 'Connection security' option under the 'Settings' section. The main area shows the 'Firewall rules' section with a note about allowing access to Azure services (ON). It also shows sections for VNET rules and SSL settings, both currently empty.

2. In the firewall rules for the Azure Database for MySQL, you can specify a single IP address or a range of addresses. If you want to limit the rule to a single IP address, type the same address in the Start IP and End IP fields. Opening the firewall enables administrators, users, and application to access any database on the MySQL server to which they have valid credentials.

The screenshot shows the 'mydemoserver - Connection security' page in the Azure portal. On the left, a sidebar lists various server management options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Connection security (which is selected), Connection strings, Server parameters, Replication, Pricing tier, Properties, Locks, and Export template. Under Security, it includes Advanced Threat Protection, Intelligent Performance, Query Performance Insight, and Performance recommendations. The main content area is titled 'Firewall rules'. It contains a note about network environments not reporting actual public-facing IP addresses. A switch labeled 'Allow access to Azure services' is set to 'OFF'. Below this is a table of firewall rules:

| Rule name                         | Start IP address | End IP address  |
|-----------------------------------|------------------|-----------------|
| ClientIPAddress_2019-9-4_13-47-46 | 123.123.123.123  | 123.123.123.123 |
| RangeOfAddresses                  | 123.123.123.0    | 123.123.123.255 |

Below the table are sections for 'VNET rules' (with a link to add existing or create new virtual networks) and 'SSL settings' (with a note about enforcing SSL connections and a switch set to 'ENABLED').

3. Click Save on the toolbar to save this server-level firewall rule. Wait for the confirmation that the update to the firewall rules is successful.

Reference:

<https://docs.microsoft.com/en-us/azure/mysql/howto-manage-firewall-using-portal#create-a-server-level-firewall-rule-in-the-azure-portal>

## Question: 359

CertyIQ

Your company has a release pipeline in an Azure DevOps project. You plan to deploy to an Azure Kubernetes Services (AKS) cluster by using the Helm package and deploy task. You need to install a service in the AKS namespace for the planned deployment. Which service should you install?

- A. Azure Container Registry
- B. Chart
- C. Kubectl
- D. Tiller

Answer: D

Explanation:

Before you can deploy Helm in an RBAC-enabled AKS cluster, you need a service account and role binding for the Tiller service.

Incorrect Answers:

C: Kubectl is a command line interface for running commands against Kubernetes clusters.

Reference:

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

## Question: 360

CertyIQ

### SIMULATION -

You need to create a virtual machine template in an Azure DevTest Labs environment named az400-123456789-dtl1. The template must be based on Windows Server 2019 Datacenter. Virtual machines created from the template must include the selenium tool and the Google Chrome browser.

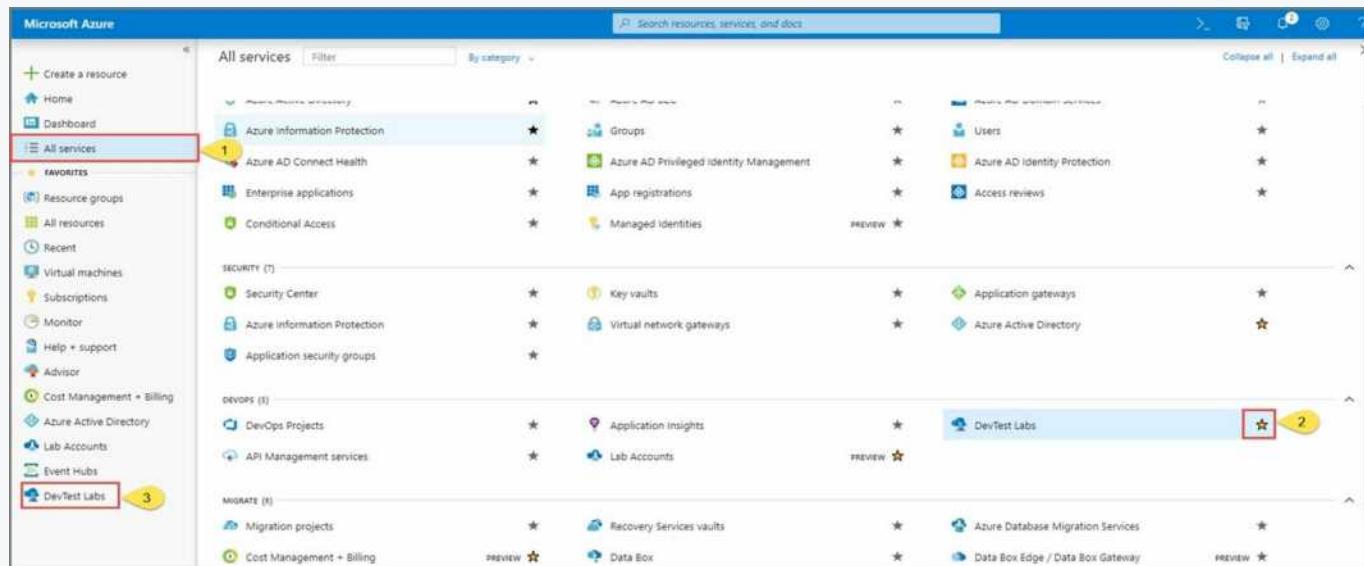
To complete this task, sign in to the Microsoft Azure portal.

### Answer: B

#### Explanation:

**Answer is no Configure a build policy instead**

1. Open Microsoft Azure Portal
2. Select All Services, and then select DevTest Labs in the DEVOPS section.



3. From the list of labs, select the az400-123456789-dtl1 lab.
4. On the home page for your lab, select + Add on the toolbar.
5. Select the Windows Server 2019 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.

#### Reference:

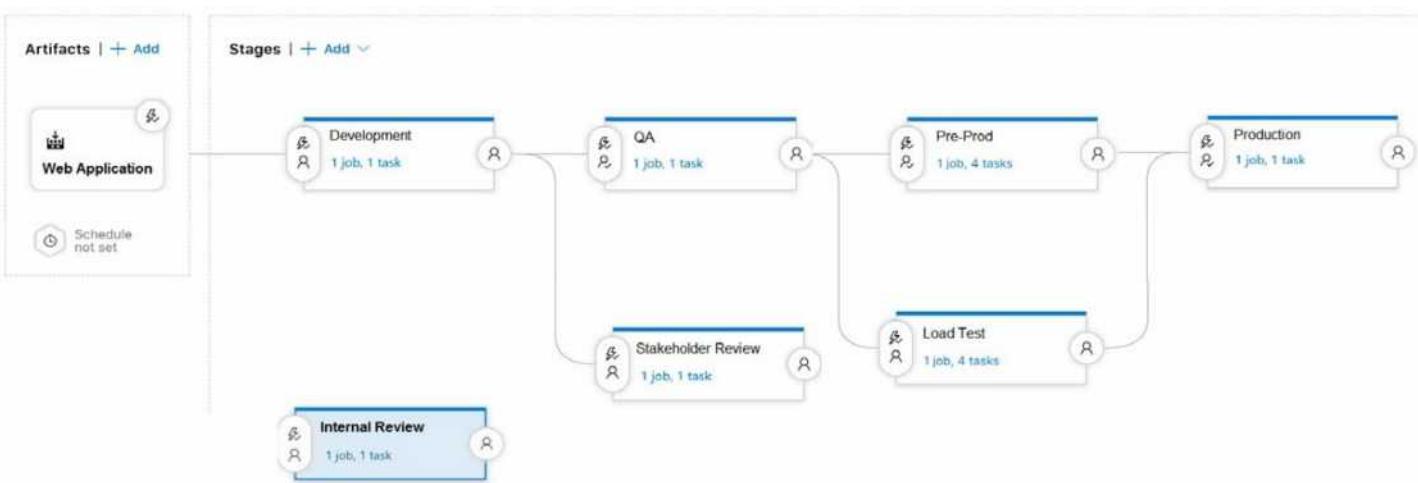
<https://docs.microsoft.com/bs-cyrl-ba/azure//lab-services/devtest-lab-vm-powershell>

## Question: 361

CertyIQ

### HOTSPOT -

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.

Hot Area:

## Answer Area

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:**

## Answer Area

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:

7

The web application artifact

## Question: 362

CertyIQ

DRAG DROP -

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.

Select and Place:

### 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

Ten virtual machines hosted in Azure:

A deployment group

A management group

Ten virtual machines hosted in  
an on-premises data center environment:

A deployment group

A resource group

Application roles

### Explanation:

Box 1: A deployment group -

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

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

Box 2: A deployment group -

Reference:

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

## Question: 363

CertyIQ

You plan to use Terraform to deploy an Azure resource group from a Windows system.

You need to install the required frameworks to support the planned deployment.

Which two frameworks should you install? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

### Answer: BD

### Explanation:

You can use the combination of Terraform and Yeoman. Terraform is a tool for creating infrastructure on Azure. Yeoman makes it easy to create Terraform modules.

Terratest provides a collection of helper functions and patterns for common infrastructure testing tasks, like making HTTP requests and using SSH to access a specific virtual machine. The following list describes some of the major advantages of using Terratest:

- ⇒ Convenient helpers to check infrastructure - This feature is useful when you want to verify your real infrastructure in the real environment.
- ⇒ Organized folder structure - Your test cases are organized clearly and follow the standard Terraform module folder structure.
- ⇒ Test cases are written in Go - Many developers who use Terraform are Go developers. If you're a Go

developer, you don't have to learn another programming language to use Terratest.

⇒ Extensible infrastructure - You can extend additional functions on top of Terratest, including Azure-specific features.

Reference:

<https://docs.microsoft.com/en-us/azure/developer/terraform/create-base-template-using-yeoman> <https://docs.microsoft.com/en-us/azure/developer/terraform/test-modules-using-terratest>

## Question: 364

CertyIQ

SIMULATION -

You plan to implement a CI/CD strategy for an Azure Web App named az400-123456789-main.

You need to configure a staging environment for az400-123456789-main.

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

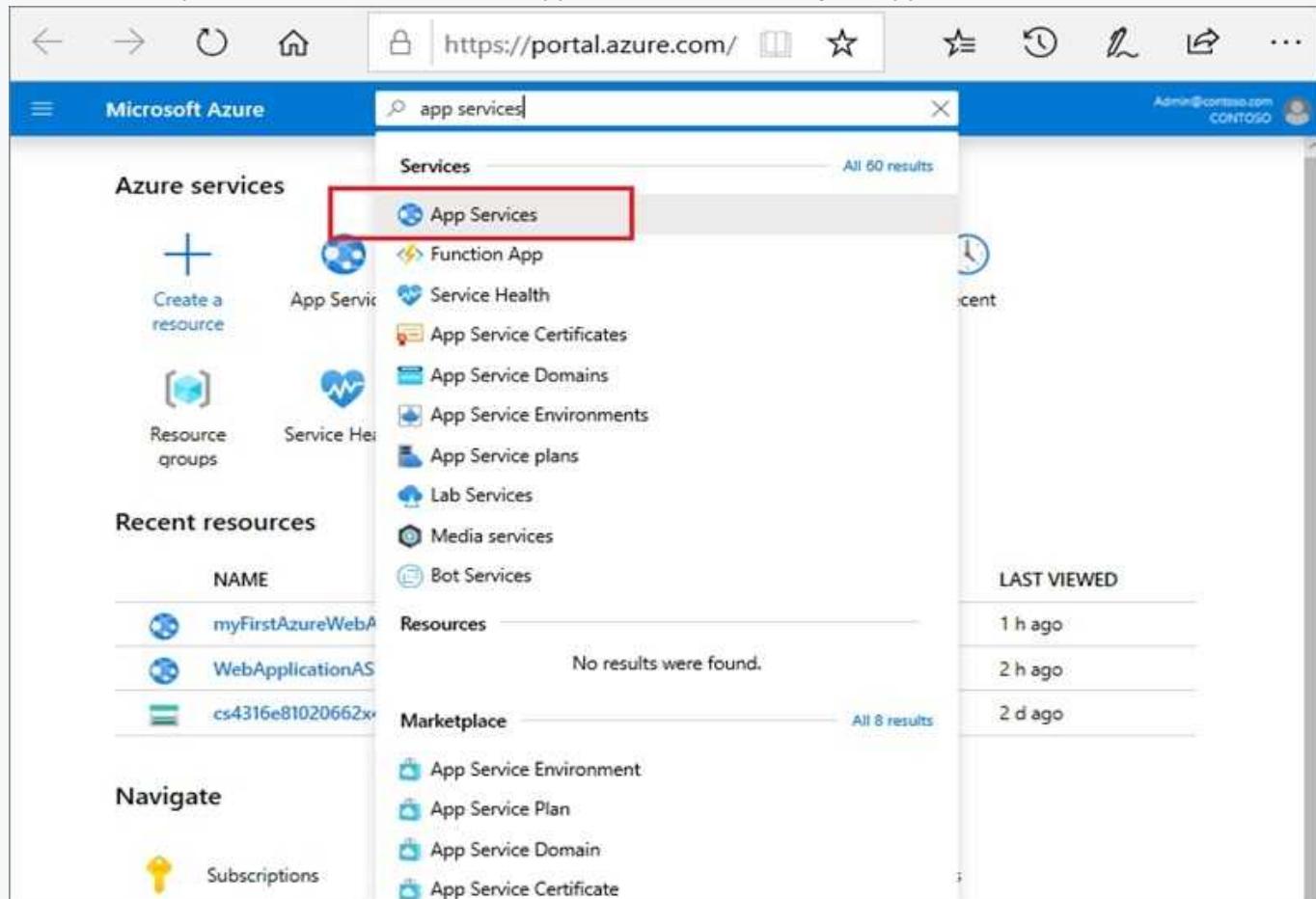
Answer:

See explanation below.

Explanation:

Add a slot -

1. In the Azure portal, search for and select App Services and select your app az400-123456789-main.



The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar with the text 'app services'. Below the search bar, the 'Services' section is displayed with a list of items. The 'App Services' item is highlighted with a red box. Other items in the list include 'Function App', 'Service Health', 'App Service Certificates', 'App Service Domains', 'App Service Environments', 'App Service plans', 'Lab Services', 'Media services', and 'Bot Services'. To the left of the main content area, there is a sidebar with sections for 'Azure services' (Create a resource, App Services, Resource groups, Service Health), 'Recent resources' (myFirstAzureWebA, WebApplicationAS, cs4316e81020662x), and 'Navigate' (Subscriptions). On the right side, there is a 'LAST VIEWED' section with entries for '1 h ago', '2 h ago', and '2 d ago'.

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

my-demo-app - Deployment slots

App Service

Save Discard Add Slot Swap Refresh

You haven't added any deployment slots. Click here to get started.

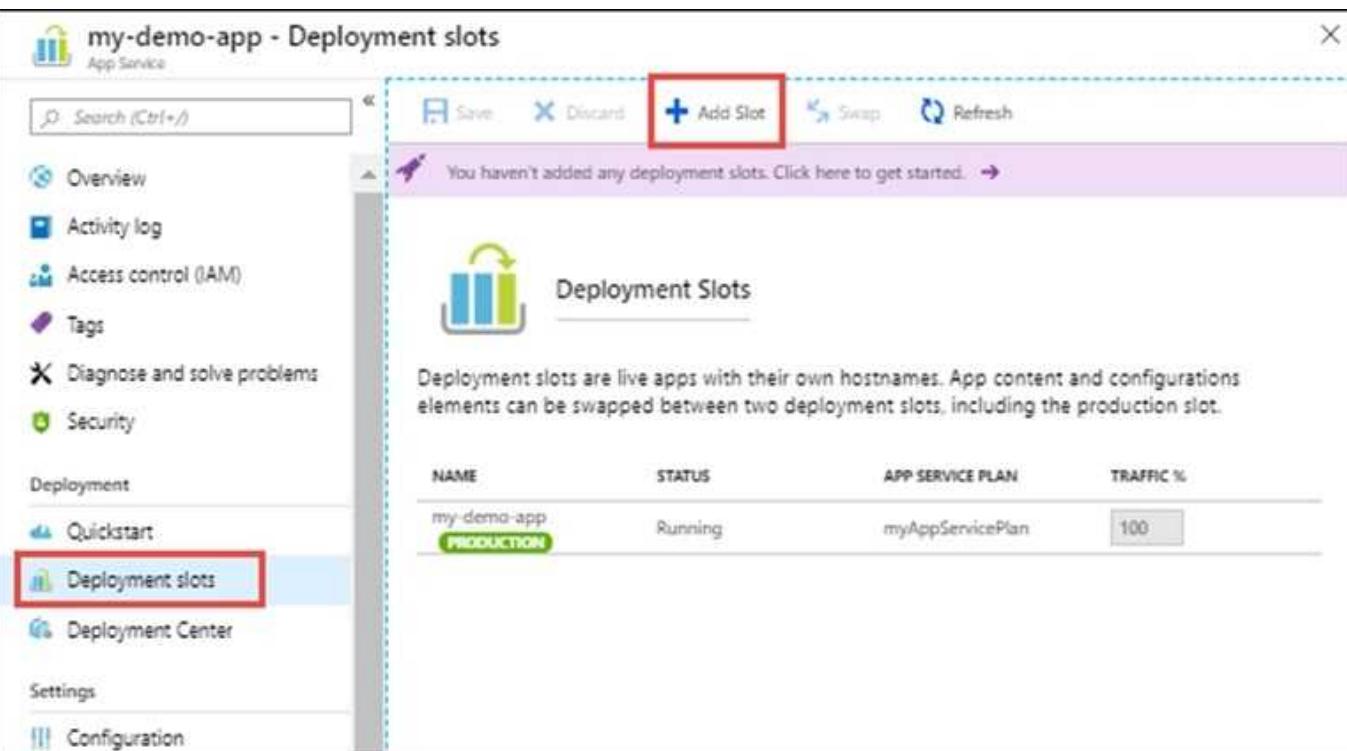
Deployment Slots

Deployment slots are live apps with their own hostnames. App content and configurations elements can be swapped between two deployment slots, including the production slot.

| NAME                             | STATUS  | APP SERVICE PLAN | TRAFFIC % |
|----------------------------------|---------|------------------|-----------|
| my-demo-app<br><b>PRODUCTION</b> | Running | myAppServicePlan | 100       |

Search (Ctrl+ /)

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Security Deployment Quickstart Deployment slots Deployment Center Settings Configuration



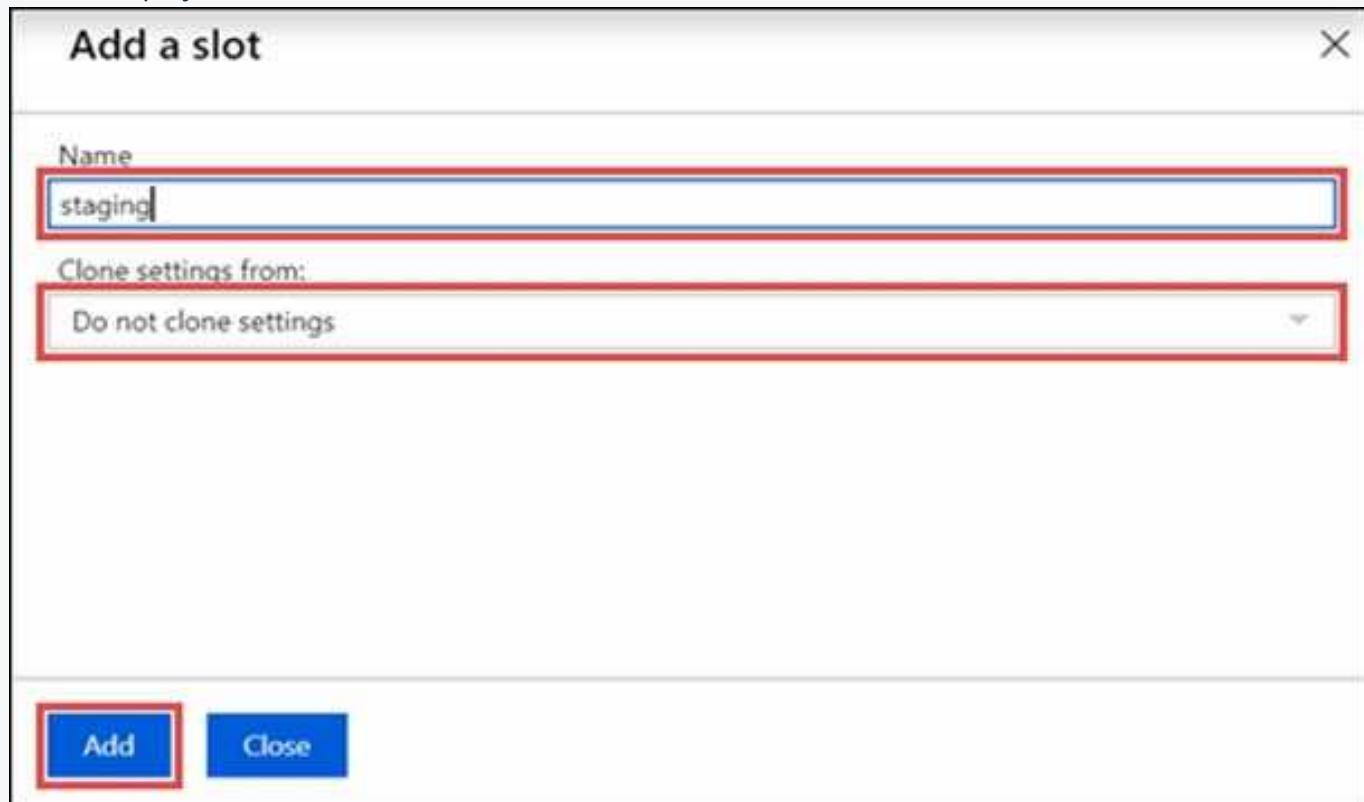
3. In the Add a slot dialog box, give the slot a name, and select whether to clone an app configuration from another deployment slot. Select Add to continue.

Add a slot

Name: **staging**

Clone settings from: **Do not clone settings**

Add Close



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

The screenshot shows the Azure portal interface for managing deployment slots. On the left, a sidebar lists various options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Deployment, Quickstart, Deployment slots (which is selected and highlighted in blue), Deployment Center, Settings, and Configuration. The main content area is titled 'Deployment Slots' and contains a brief description: 'Deployment slots are live apps with their own hostnames. App content and configurations elements can be swapped between two deployment slots, including the production slot.' Below this is a table with columns: NAME, STATUS, APP SERVICE PLAN, and TRAFFIC %. Two rows are present: 'my-demo-app' (PRODUCTION) and 'my-demo-app-staging'. The 'my-demo-app-staging' row is highlighted with a red box.

Reference:

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

## Question: 365

CertyIQ

SIMULATION -

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 explanation below.

#### Explanation:

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

The screenshot shows the 'Automatic tuning' configuration page for an Azure SQL Database. At the top, there's a message: 'Azure SQL Database built-in intelligence automatically tunes your databases to optimize performance. Click here to learn more about automatic tuning.' Below this, there's an 'Inherit from:' dropdown with 'Server' selected. There are three tabs: 'Server', 'Azure defaults', and 'Don't inherit'. A note says: 'The database is inheriting automatic tuning configuration from the server. You can set the configuration to be inherited by going to Server tuning settings.' Under 'Configure the automatic tuning options:', there are three sections: 'FORCE PLAN', 'CREATE INDEX', and 'DROP INDEX'. Each section has a 'DESIRED STATE' table with columns 'ON', 'OFF', and 'INHERIT'. For all three, 'ON' is the current state and 'INHERIT' is selected. At the bottom left is an 'Apply' button.

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/azure-sql/database/automatic-tuning-enable>

## Question: 366

CertyIQ

HOTSPOT -

You use Azure Pipelines to manage the build and deployment of apps.

You are planning the release strategies for a new app.

You need to choose strategies for the following scenarios:

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

- Code will be deployed to enable functionality that will be available in later releases of the app.
- When a new release occurs, the existing deployment will remain active to minimize recovery time if a return to the previous version is required.

Which strategy should you choose for each scenario? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Hot Area:

### 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        |

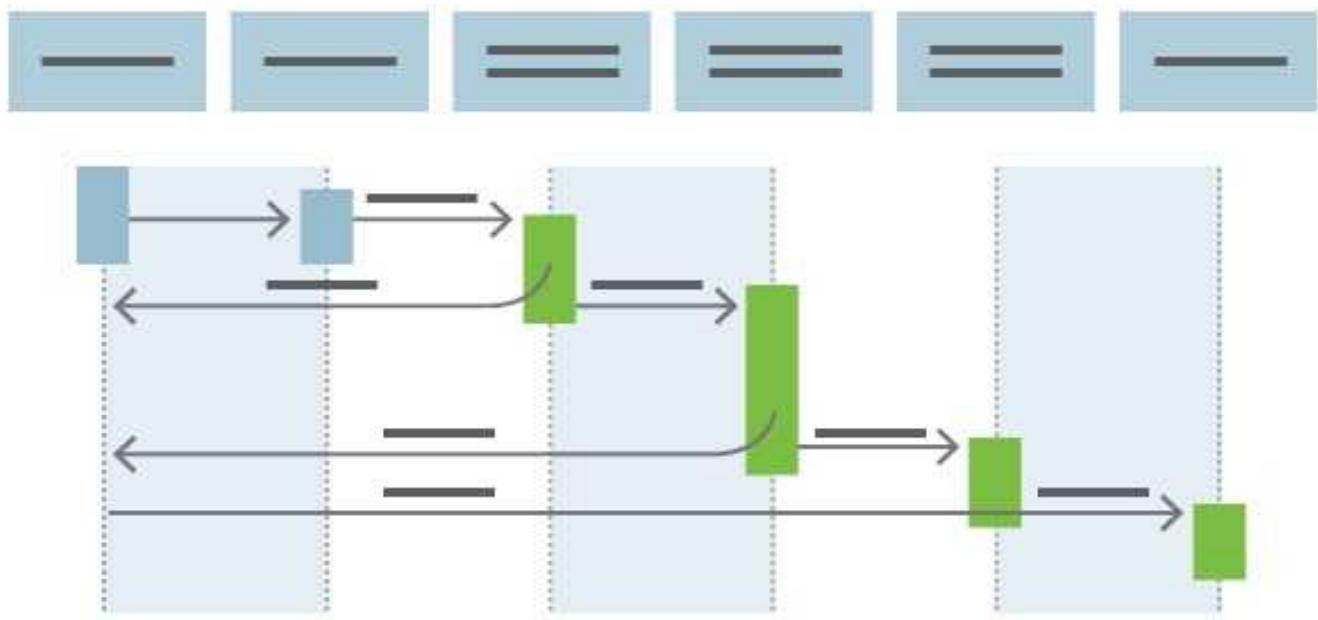
When a new release occurs, the existing deployment will remain active to minimize recovery time if a return to the previous version is required:

|                      |
|----------------------|
| ▼                    |
| Progressive exposure |
| Blue/green           |
| Feature flags        |

### Explanation:

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 mean 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 ever 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-appgateway-or-trafficmanager-4490bce29cb>

**Question: 367**

CertyIQ

DRAG DROP -

You have a project in Azure DevOps.

You need to associate an automated test to a test case.

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

Select and Place:

| Actions                                           | Answer Area                                                                         |
|---------------------------------------------------|-------------------------------------------------------------------------------------|
| Debug the project                                 |                                                                                     |
| Create a test project                             |                                                                                     |
| Create a work item                                |    |
| Check in a project to the Azure DevOps repository |  |
| Add the automated test to a build pipeline        |                                                                                     |

**Answer:**

| Actions                                           | Answer Area                                                                         |
|---------------------------------------------------|-------------------------------------------------------------------------------------|
| Debug the project                                 | Create a test project                                                               |
| Create a test project                             | Check in a project to the Azure DevOps repository                                   |
| Create a work item                                |  |
| Check in a project to the Azure DevOps repository |  |
| Add the automated test to a build pipeline        | Add the automated test to a build pipeline                                          |

**Explanation:**

The process to associate an automated test with a test case is:

1. Create a test project containing your automated test. What types of tests are supported?
2. Check your test project into an Azure DevOps or Team Foundation Server (TFS) repository.

3. Create a build pipeline for your project, ensuring that it contains the automated test. What are the differences if I am still using a XAML build?

4. Use Visual Studio Enterprise or Professional 2017 or a later version to associate the automated test with a test case as shown below. The test case must have been added to a test plan that uses the build you just defined.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/test/associate-automated-test-with-test-case>

### Question: 368

CertyIQ

DRAG DROP -

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.

Select and Place:

#### 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 Area

|  |
|--|
|  |
|  |
|  |

Answer:

## 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 Area

Create a service principal in Azure Active Directory (Azure AD).

Configure RBAC roles in the cluster.

Add a Helm package and deploy a task to the deployment pipeline.

## Explanation:

1. Create a service principal in Azure Active Directory
2. Configure RBAC roles in the cluster
3. Add a helm package and deploy a task to the deployment pipeline

## Question: 369

CertyIQ

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 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.

Reference:

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

## Question: 370

CertyIQ

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:

Not such option as gates timeout in pre-deployment approvals. Pre-deployment approvals are for manual approvals and gates are for automatic approvals

### Question: 371

CertyIQ

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

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

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

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

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

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

Solution: From Pre-deployment conditions, you modify the Timeout setting for pre-deployment approvals.

Does this meet the goal?

A. Yes

B. No

#### Answer: A

#### Explanation:

Pre-deployment approvals is where setting is changed for timeout.

### Question: 372

CertyIQ

DRAG DROP -

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.

Select and Place:

### 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:

Blue/Green deployment

### Explanation:

App1: Canary deployment -

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

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

## App2:"Blue-green deployment

also gives us a fast way to do a rollback. If anything goes wrong in the green environment, then we just switch the router back to the blue environment."

### Question: 373

CertyIQ

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.

Reference:

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

### Question: 374

CertyIQ

DRAG DROP -

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 on 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.

Select and Place:

**Actions****Answer Area**

Create an Azure Automation account.

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

Create a .zip file and upload it to Azure Blob storage.



Onboard the virtual machines to the Azure Automation account.

Compile the Desired State Configuration (DSC) configuration.

**Answer:****Actions****Answer Area**

Create an Azure Automation account.

Create an Azure Automation account.

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

Compile the Desired State Configuration (DSC) configuration.

Create a .zip file and upload it to Azure Blob storage.



Onboard the virtual machines to the Azure Automation account.

Onboard the virtual machines to the Azure Automation account.

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

Compile the Desired State Configuration (DSC) configuration.

**Explanation:**

1. Create Az Automation
2. Upload/Compile DSC Configuration
3. Register or Onboard VM to be Managed
4. Install (dsc ) extension

<https://docs.microsoft.com/en-us/azure/automation/tutorial-configure-servers-desired-state#compile-a-configuration-into-a-node-configuration>

**Question: 375****CertyIQ**

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. The build process requires access to resource files located in an on-premises file system.

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

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

What should you do?

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

**Answer: C**

**Explanation:**

### C - Microsoft-hosted vs. self-hosted parallel jobs

If you want to run your jobs on machines that Microsoft manages, use Microsoft-hosted parallel jobs. Your jobs will run on Microsoft-hosted agents.

If you want Azure Pipelines to orchestrate your builds and releases, but use your own machines to run them, use self-hosted parallel jobs. For self-hosted parallel jobs, you'll start by deploying our self-hosted agents on your machines. You can register any number of these self-hosted agents in your organization.

**Question: 376**

**CertyIQ**

SIMULATION -

You need to ensure that an Azure web app named az400-123456789-main supports rolling upgrades. The solution must ensure that only 10 percent of users who connect to az400-123456789-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 explanation 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.

Add a slot

Name:

Clone settings from:

**Add** **Close**

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.

my-demo-app - Deployment slots

Deployment Slots

Deployment slots are live apps with their own hostnames. App content and configurations elements can be swapped between two deployment slots, including the production slot.

| NAME                             | STATUS  | APP SERVICE PLAN | TRAFFIC % |
|----------------------------------|---------|------------------|-----------|
| my-demo-app<br><b>PRODUCTION</b> | Running | myAppServicePlan | 100       |
| my-demo-app-staging              | Running | myAppServicePlan | 0         |

6. Change TRAFFIC % to 10

Reference:

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

**Question: 377**

CertyIQ

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>

## Question: 378

**CertyIQ**

HOTSPOT -

You have a project in 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.

Hot Area:

## Answer Area

```
"resources": [
 {
 "apiversion": "2018-05-01",
 "name" : "secrets",
 "type": "Microsoft.KeyVault/vaults",
 "Microsoft.Resources/deployments",
 "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')]"
 }
 }
}
}
],
},
```

Answer:

## Answer Area

```
"resources": [
 {
 "apiVersion": "2018-05-01",
 "name" : "secrets",
 "type": "Microsoft.KeyVault/vaults",
 "Microsoft.Resources/deployments",
 "Microsoft.Subscription/subscriptions"
 },
 {
 "properties": {
 "mode" : "Incremental",
 "deployment"
 "template"
 "templateLink"
 }
 }
],
{
 "contentVersion": "1.0.0.0",
 "uri" : "[uri(parameters('_artifactsLocation'),
 concat('./nested/sqlserver.json',
 parameters('_artifactsLocationSasToken')))]"
},
{
 "parameters": {
 "secret": {
 "reference": {
 "keyVault": {
 "id": "[resourceId(parameters('vaultSubscription'),
 parameters('vaultResourceGroupName'),
 'Microsoft.KeyVault/vaults',
 parameters('vaultName'))]"
 },
 "secretName": "[parameters('secretName')]"
 }
 }
 }
}
],
]
,
```

### Explanation:

Box 1: "Microsoft.Resources/deployments"

Reference a secret with dynamic ID. You need to reference a key vault secret that varies based on the current deployment.

Example:

```
"resources": [
```

```
 "apiVersion": "2018-05-01",
 "name": "dynamicSecret",
 "type": "Microsoft.Resources/deployments",
 "properties": {
 "mode": "Incremental",
 "templateLink": "
```

Box 2: "templateLink"

In your parent template, you add the linked template and pass in a parameter that contains the dynamically generated resource ID.

Reference:

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

## Question: 379

CertyIQ

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

The company uses ServiceNow for change management.

You need to ensure that a change request is processed before any components can be deployed to the production environment.

What are two ways to integrate ServiceNow into the Azure DevOps release pipeline? Each correct answer presents a complete solution.

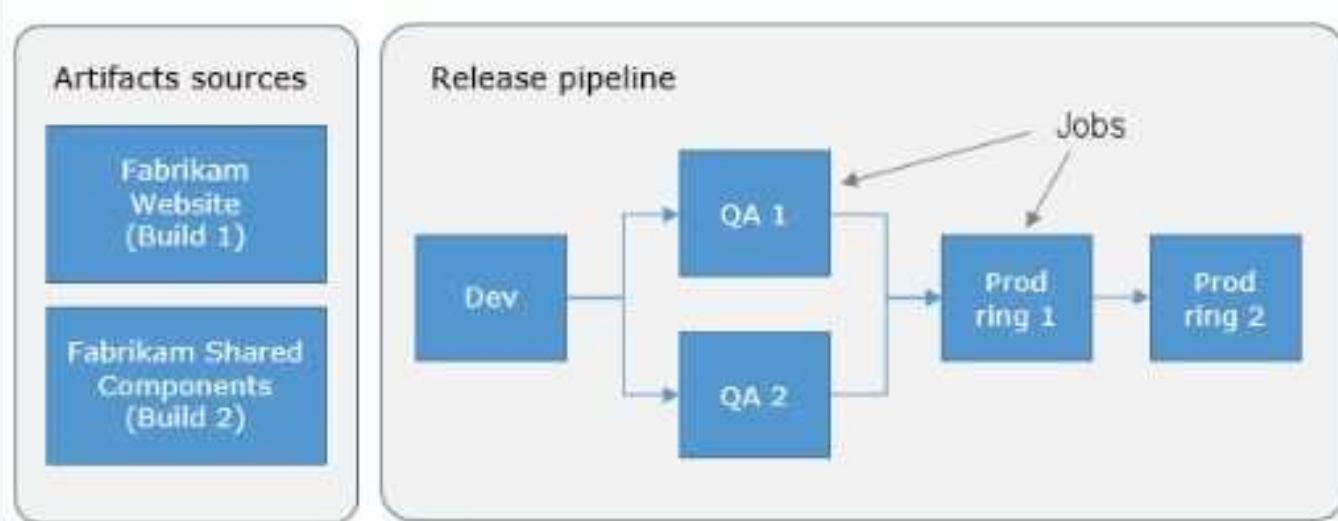
NOTE: Each correct selection is worth one point.

- A. Define a deployment control that invokes the ServiceNow REST API.
- B. Define a pre-deployment gate before the deployment to the Prod stage.
- C. Define a deployment control that invokes the ServiceNow SOAP API.
- D. Define a post-deployment gate after the deployment to the QA stage.

**Answer: BD**

**Explanation:**

An example of a release pipeline that can be modeled through a release pipeline is shown below:



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

Reference:

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

## Question: 380

CertyIQ

Your company develops an application named App1 that is deployed in production.

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

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

What should you do?

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

**Answer: A****Explanation:**

Feature flags support a customer-first DevOps mindset, to enable (expose) and disable (hide) features in a solution, even before they are complete and ready for release.

**Incorrect Answers:**

C: Branch policies are an important part of the Git workflow and enable you to:

- ⇒ Isolate work in progress from the completed work in your master branch
- ⇒ Guarantee changes build before they get to master

**Reference:**

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

**CertyIQ****Question: 381**

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.

**Reference:**

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

**CertyIQ****Question: 382**

You are developing an iOS application by using Azure DevOps.

You need to test the application manually on 10 devices without releasing the application to the public.

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

NOTE: Each correct selection is worth one point.

- A. Create a Microsoft Intune device compliance policy.
- B. Deploy a certificate from an internal certification authority (CA) to each device.
- C. Register the application in the iTunes store.

- D. Onboard the devices into Microsoft Intune.
- E. Distribute a new release of the application.
- F. Register the IDs of the devices in the Apple Developer portal.

**Answer: EF**

**Explanation:**

F: register device to Apple

download new provisioning profile from Apple

resign with the new profile (which is from Apple, not private CA, so B is incorrect)

E: Distribute a new release

**CertyIQ**

**Question: 383**

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. Create an active subscription in App Center Test.
- C. Create an unsigned build.
- D. Add the device owner to the collaborators group.

**Answer: A**

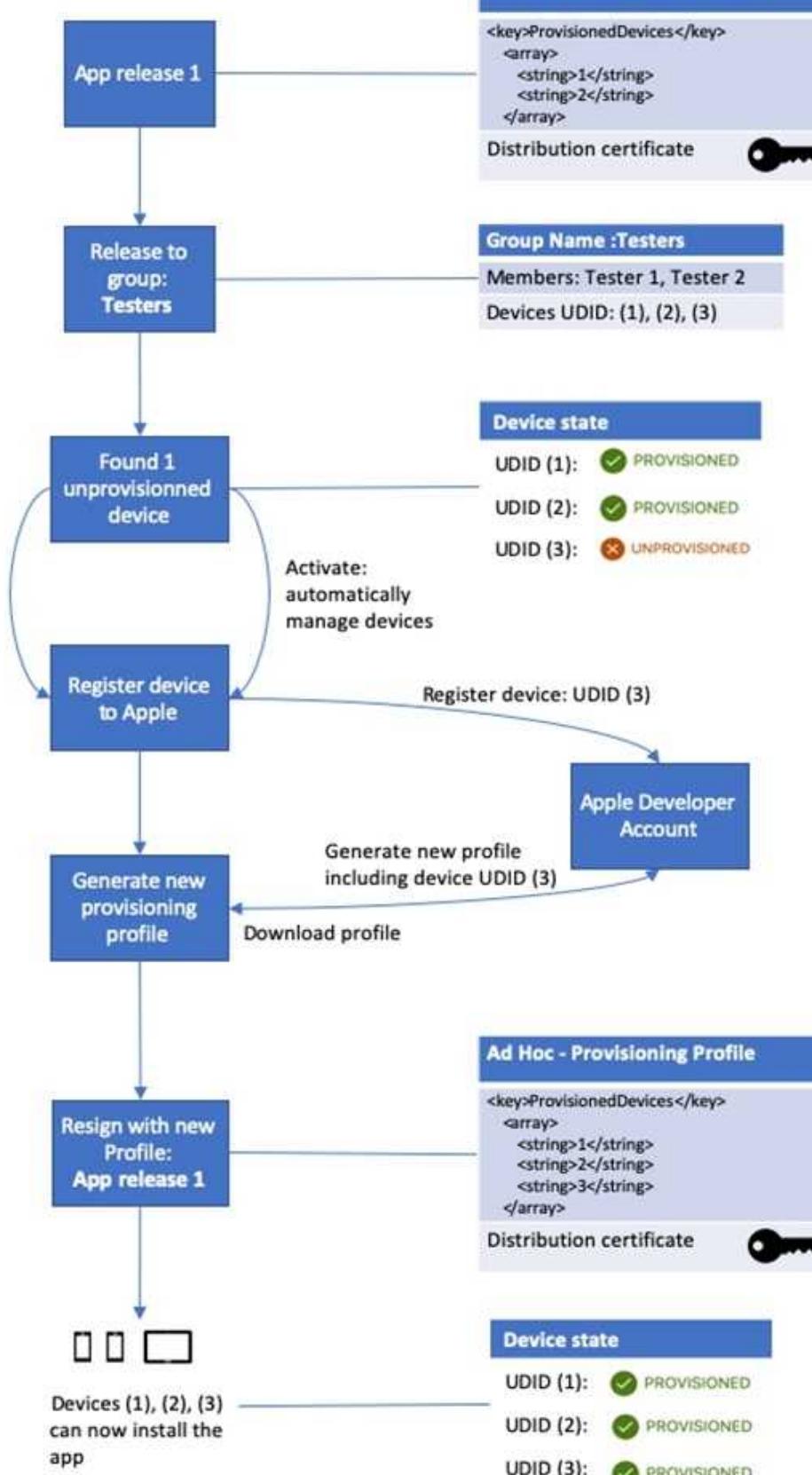
**Explanation:**

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



**App Center**  
[install.appcenter.ms/apps](http://install.appcenter.ms/apps)

Manual: click on  
register devices



Incorrect Answers:

C: The application build must be signed.

D: The device owner does not need to be added.

Reference:

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

CertyIQ

### Question: 384

SIMULATION -

You plan to deploy a website that will be hosted in two Azure regions.

You need to create an Azure Traffic Manager profile named az400123456789n1-tm in a resource group named RG1lod123456789. 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 explanation 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: az400123456789n1-tm -

Routing method: Geographic -

Resource group: RG1lod123456789 -

# Create Traffic Manager profile

## \* Name

 ✓

.trafficmanager.net

## Routing method

 ✓

## \* Subscription

## \* Resource group

 Create new  Use existing ✓

## \* Resource group location

 ✓

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-azure-traffic-manager/>

## Question: 385

CertyIQ

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

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

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

NOTE: Each correct selection is worth one point.

- A. a deployment group
- B. a Microsoft-hosted agent
- C. service hooks

D. a self-hosted agent

E. an External Git service connection

**Answer: DE**

**Explanation:**

E: GitLab CI/CD can be used with GitHub or any other Git server such as BitBucket. Instead of moving your entire project to GitLab, you can connect your external repository to get the benefits of GitLab CI/CD.

Note: When a pipeline uses a remote, 3rd-party repository host such as Bitbucket Cloud, the repository is configured with webhooks that notify Azure Pipelines

Server or TFS when code has changed and a build should be triggered. Since on-premises installations are normally protected behind a firewall, 3rd-party webhooks are unable to reach the on-premises server. As a workaround, you can use the External Git repository type which uses polling instead of webhooks to trigger a build when code has changed.

Reference:

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

**Question: 386**

CertyIQ

HOTSPOT -

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.

Hot Area:

## Answer Area

Branch lifetime:

|             |   |
|-------------|---|
|             | ▼ |
| Long-lived  | ▼ |
| Short-lived | ▼ |

Branch type:

|             |   |
|-------------|---|
|             | ▼ |
| Master      | ▼ |
| Feature     | ▼ |
| Integration | ▼ |

**Answer:**

# Answer Area

Branch lifetime:

|             |   |
|-------------|---|
|             | ▼ |
| Long-lived  |   |
| Short-lived |   |

Branch type:

|             |   |
|-------------|---|
|             | ▼ |
| Master      |   |
| Feature     |   |
| Integration |   |

## Explanation:

Branch lifetime: Short-lived -

Branch type: Feature -

Feature branches are used when developing a new feature or enhancement which has the potential of a development lifespan longer than a single deployment.

When starting development, the deployment in which this feature will be released may not be known. No matter when the feature branch will be finished, it will always be merged back into the master branch.

## Reference:

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

## Question: 387

CertyIQ

You have a project in Azure DevOps.

You plan to deploy a self-hosted agent by using an unattended configuration script.

Which two values should you define in the configuration script? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. authorization credentials
- B. the project name
- C. the deployment group name
- D. the organization URL
- E. the agent pool name

## Answer: AD

## Explanation:

Unattended config:

The agent can be set up from a script with no human intervention. You must pass --unattended and the answers to all questions.

To configure an agent, it must know the URL to your organization or collection and credentials of someone

authorized to set up agents. All other responses are optional.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-windows>

CertyIQ

### Question: 388

HOTSPOT -

You have an Azure virtual machine named VM1 that runs Linux.

You plan to deploy the Desired State Configuration (DSC) extension to VM1.

You need to grant the Log Analytics agent the appropriate directory permissions.

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

`setfacl -m u:omsagent:`

|     |      |
|-----|------|
| r   | /lib |
| x   | /etc |
| rx  | /tmp |
| rwx | /usr |

Answer:

### Answer Area

`setfacl -m u:omsagent:`

|     |      |
|-----|------|
| r   | /lib |
| x   | /etc |
| rx  | /tmp |
| rwx | /usr |

### Explanation:

Box 1: rwx -

The Log Analytics agent for Linux runs as the omsagent user. To grant >write permission to the omsagent user, run the command `setfacl -m u:omsagent:rwx /tmp`.

Box 2: /tmp -

Deploying DSC to a Linux node uses the /tmp folder.

Reference:

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

CertyIQ

### Question: 389

HOTSPOT -

You are using PowerShell to administer Azure Log Analytics workspaces.

You need to list the available workspaces and their properties.

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

|                        |                    |                                                             |
|------------------------|--------------------|-------------------------------------------------------------|
| Get-AzResource         | -ResourceGroupName | Microsoft.OperationalInsights/workspaces - ExpandProperties |
| Get-AzResourceGroup    | -ResourceId        |                                                             |
| Get-AzResourceProvider | -ResourceType      |                                                             |

Answer:

## Answer Area

|                        |                    |                                                             |
|------------------------|--------------------|-------------------------------------------------------------|
| Get-AzResource         | -ResourceGroupName | Microsoft.OperationalInsights/workspaces - ExpandProperties |
| Get-AzResourceGroup    | -ResourceId        |                                                             |
| Get-AzResourceProvider | -ResourceType      |                                                             |

### Explanation:

Box 1: Get-AzResource -

Use the following command to examine the access control mode for all workspaces in the subscription:

PowerShell -

```
Get-AzResource -ResourceType Microsoft.OperationalInsights/workspaces -ExpandProperties | foreach
$_.Name + ":" +
$.Properties.features.enableLogAccessUsingOnlyResourcePermissions
```

Box 2: -ResourceType -

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/manage-access>

## Question: 390

CertyIQ

You have Azure Pipelines and GitHub integrated as a source code repository.

The build pipeline has continuous integration enabled.

You plan to trigger an automated build whenever code changes are committed to the repository.

You need to ensure that the system will wait until a build completes before queuing another build.

What should you implement?

- A. path filters
- B. batch changes**
- C. scheduled builds
- D. branch filters

Answer: B

### Explanation:

Batching CI runs -

If you have many team members uploading changes often, you may want to reduce the number of runs you start. If you set batch to true, when a pipeline is running, the system waits until the run is completed, then starts another run with all changes that have not yet been built.

Example:

```
specific branch build with batching
trigger:
batch: true
```

branches:

include:

- master

To clarify this example, let us say that a push A to master caused the above pipeline to run. While that pipeline is running, additional pushes B and C occur into the repository. These updates do not start new independent runs immediately. But after the first run is completed, all pushes until that point of time are batched together and a new run is started.

Reference:

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

CertyIQ

### Question: 391

You are using GitHub as a source code repository.

You create a client-side Git hook on the commit-msg event. The hook requires that each commit message contain a custom work item tag.

You need to make a commit that does not have a work item tag.

Which git commit parameter should you use?

- A. --squash
- B. --no-verify
- C. --message ''
- D. --no-post-rewrite

### Answer: B

#### Explanation:

The commit-msg hook is invoked by git-commit and git-merge, and can be bypassed with the --no-verify option.

Reference:

<https://git-scm.com/docs/githooks>

CertyIQ

### Question: 392

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

### Answer: A

#### Explanation:

Distribute a new release.

When you distribute a new release to a group that doesn't have automatic device management enabled, a Devices step is part of the wizard. The step checks if you have unprovisioned devices in the distribution group; if this happens, you can check the Register devices and re-sign app checkbox. App Center then runs three operations for you:

1. Register new device IDs in the Apple Developer portal.
2. Add the devices to the provisioning profile and download it.
3. Re-sign the uploaded binary so that all testers can install it.

Reference:

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

CertyIQ

### Question: 393

DRAG DROP -

You need to deploy Internet Information Services (IIS) to an Azure virtual machine that runs Windows Server 2019. How should you complete the Desired State Configuration (DSC) configuration script? To answer, drag the appropriate values to the correct locations. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

#### Values

Configuration

DependsOn

File

IncludeAllSubFeature

WindowsFeature

#### Answer Area

```
MyDsc {
 Node 'Server1' {
 [] MyConfigDetail {
 Ensure = 'Present'
 Name = 'Web-Server'
 }
 }
}
```

### Answer:

#### Values

Configuration

DependsOn

File

IncludeAllSubFeature

WindowsFeature

#### Answer Area

```
Configuration MyDsc {
 Node 'Server1' {
 [] WindowsFeature MyConfigDetail {
 Ensure = 'Present'
 Name = 'Web-Server'
 }
 }
}
```

### Explanation:

Box 1: Configuration -  
Configuration Example:

Configuration Sample -

Node localhost, server02 -

Box 2: WindowsFeature -  
Example:

WindowsFeature RoleExample -

```
Ensure = "Present"
Alternatively, to ensure the role is uninstalled, set Ensure to "Absent"
Name = "Web-Server" # Use the Name property from Get-WindowsFeature
```

The WindowsFeature resource in Windows PowerShell Desired State Configuration (DSC) provides a mechanism to ensure that roles and features are added or removed on a target node.

Reference:

<https://docs.microsoft.com/en-us/powershell/dsc/reference/resources/windows/windowsfeatureresource> <https://docs.microsoft.com/en-us/powershell/dsc/managing-nodes/apply-get-test>

## Question: 394

CertyIQ

HOTSPOT -

You plan to use Desired State Configuration (DSC) to maintain the configuration of a server that runs Windows Server 2019.

The server must have the following features installed:

- ⇒ A web server
- ⇒ An email server

How should you complete the DSC configuration file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

```
configuration RequiredFeatures
{
 Import-DscResource -ModuleName PSDesiredStateConfiguration
 Node localhost
 {
 WindowsFeatureSet RequiredWindowsFeatures
 {
 Name = @("Mail-Server", "IIS")
 Name = @("SMTP-Server", "IIS")
 Name = @("Mail-Server", "Web-Server")
 Name = @("SMTP-Server", "Web-Server")
 Ensure = 'Present'
 Install
 Ensure
 Enforce
 Required
 IncludeAllSubFeature = $true
 }
 }
}
```

Answer:

```

configuration RequiredFeatures
{
 Import-DscResource -ModuleName PSDesiredStateConfiguration

 Node localhost
 {
 WindowsFeatureSet RequiredWindowsFeatures
 {
 Name
 = @("Mail-Server", "IIS")
 = @("SMTP-Server", "IIS")
 = @("Mail-Server", "Web-Server")
 = @("SMTP-Server", "Web-Server")

 Ensure
 = 'Present'

 Install
 Ensure
 Enforce
 Required

 IncludeAllSubFeature = $true
 }
 }
}

```

#### Explanation:

Box 1: = @("SMTP-Server", "Web-Server")

The following configuration ensures that the Web-Server (IIS) and SMTP (email) Server features, and all subfeatures of each, are installed. configuration FeatureSetTest

```
Import-DscResource -ModuleName PSDesiredStateConfiguration
```

```
Node localhost -
```

```
WindowsFeatureSet WindowsFeatureSetExample
```

```
Name = @("SMTP-Server", "Web-Server")
```

```
Ensure = 'Present'
```

```
IncludeAllSubFeature = $true -
```

Box 2: Ensure -

Ensure indicates whether the roles or features are added. To ensure that the roles or features are added, set this property to Present. To ensure that the roles or features are removed, set the property to Absent. The default value is Present.

Reference:

<https://docs.microsoft.com/en-us/powershell/dsc/reference/resources/windows/windowsFeatureSetResource>

### Question: 395

CertyIQ

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. Register the devices on the Apple Developer portal.
- B. Add the device owner to the organization in App Center.
- C. Create an unsigned build.
- D. Add the device owner to the collaborators group.

Answer: A

Explanation:

Distribute a new release.

When you distribute a new release to a group that doesn't have automatic device management enabled, a Devices step is part of the wizard. The step checks if you have unprovisioned devices in the distribution group; if this happens, you can check the Register devices and re-sign app checkbox. App Center then runs three operations for you:

1. Register new device IDs in the Apple Developer portal.
2. Add the devices to the provisioning profile and download it.
3. Re-sign the uploaded binary so that all testers can install it.

Reference:

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

### Question: 396

CertyIQ

Your company uses Azure Artifacts for package management.

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

Which repository type should you use as an upstream source?

- A. npmjs.org
- B. PyPI
- C. Maven Central
- D. third-party trusted Python

**Answer: B****Explanation:**

Get started with Python packages in Azure Artifacts

Create a feed -

1. Select Artifacts (in the left navigation of your Azure DevOps project).
2. On the Artifacts page, select Create Feed.
3. In the Create new feed dialog box:
4. In the Name field, give the feed a name.

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

Reference:

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

**CertyIQ****Question: 397**

You have a GitHub repository that contains workflows. The workflows contain steps that execute predefined actions. Each action has one or more versions.

You need to request the specific version of an action to execute.

Which three attributes can you use to identify the version? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. the SHA-based hashes
- B. the tag
- C. the runner
- D. the branch
- E. the serial

**Answer: ABD****Explanation:**

To use a specific action version, users can configure their GitHub Actions workflow to target a tag, a commit's SHA, or a branch named for a release."

Reference

<https://docs.github.com/en/actions/creating-actions/about-custom-actions#good-practices-for-release-management>

**CertyIQ****Question: 398**

You have an Azure subscription that contains multiple Azure pipelines.

You need to deploy a monitoring solution for the pipelines. The solution must meet the following requirements:

- ⇒ Parse logs from multiple sources.
- ⇒ Identify the root cause of issues.

What advanced feature of a monitoring tool should you include in the solution?

- A. analytics
- B. synthetic monitoring
- C. directed monitoring
- D. Alert Management

**Answer: A****Explanation:**

Analytics, for sure .

<https://learn.microsoft.com/en-us/azure/devops/pipelines/reports/pipelineresult?view=azure-devops>

**CertyIQ****Question: 399**

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 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 using pipeline artifacts.

Does this meet the goal?

A. Yes

B. No

**Answer: B****Explanation:**

No" [When to use artifacts versus caching] Pipeline caching and pipeline artifacts perform similar functions but are designed for different scenarios and shouldn't be used interchangeably. [Use pipeline artifacts] when you need to take specific files produced in one job and share them with other jobs (and these other jobs will likely fail without them). [Use pipeline caching] when you want to improve build time by reusing files from previous runs (and not having these files won't impact the job's ability to run).

**CertyIQ****Question: 400**

You use GitHub for source control of .NET applications.

You need to deploy a documentation solution that meets the following requirements:

- ⇒ Documents will be written in Markdown as developers make code changes.
- ⇒ Changes to the documents will trigger the recompilation of a static website.
- ⇒ Users will access the documents from the static website.
- ⇒ Documents will be stored in a GitHub repository.

Which two tools can you use to compile the website? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Word Press

B. Jekyll

C. DocFX

D. caret

E. Medium

**Answer: BC**

### Explanation:

Doc FX makes it extremely easy to generate your developer hub with a landing page, API reference, and conceptual documentation, from a variety of sources

DOX - Best Jekyll Documentation Theme

Dox is a blazing fast and feature-rich Jekyll documentation theme that is specially crafted for project documentation. You have the flexibility to use this awesome documentation theme with both GitHub and GitLab pages along with standalone projects

<https://github.com/dotnet/docfx>

<https://themefisher.com/jekyll-documentation-themes>

CertyIQ

### Question: 401

You have an on-premises app named App1 that accesses Azure resources by using credentials stored in a configuration file.

You plan to upgrade App1 to use an Azure service principal.

What is required for App1 to programmatically sign in to Azure Active Directory (Azure AD)?

- A. the application ID, a client secret, and the object ID
- B. a client secret, the object ID, and the tenant ID
- C. the application ID, a client secret, and the tenant ID**
- D. the application ID, a client secret, and the subscription ID

Answer: C

CertyIQ

### Question: 402

HOTSPOT -

You have a virtual machine that runs Windows Server 2019 and is managed by using Desired State Configuration (DSC).

You have the following DSC configuration.

```
configuration WebConfiguration
{
 File WebsiteContent {
 Ensure = 'Present'
 SourcePath = 'c:\test\index.htm'
 DestinationPath = 'c:\inetpub\wwwroot'
 DependsOn = '[WindowsFeature]Web-Server'
 }

 WindowsFeature Web-Server
 {
 Ensure = 'Present'
 Name = 'Web-Server'
 }
}
```

You have the following Local Configuration Manager (LCM) configuration.

```
LocalConfigurationManager
{
 ConfigurationMode = "ApplyAndMonitor"
 RefreshFrequencyMins = 30
 ConfigurationModeFrequencyMins = 60
 RefreshMode = 'Push'
}
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

| Statements                                                                                                                                    | Yes                   | No                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| The Index.htm file will be copied to the C:\Test folder before the Web-Server Windows feature is installed.                                   | <input type="radio"/> | <input type="radio"/> |
| If manual changes are made to the configuration of the virtual machine, the configuration will reapply automatically.                         | <input type="radio"/> | <input type="radio"/> |
| If the Web-Server Windows feature is uninstalled from the virtual machine, the discrepancy will be reported in a log entry within 60 minutes. | <input type="radio"/> | <input type="radio"/> |

#### Answer:

| Statements                                                                                                                                    | Yes                              | No                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| The Index.htm file will be copied to the C:\Test folder before the Web-Server Windows feature is installed.                                   | <input type="radio"/>            | <input checked="" type="radio"/> |
| If manual changes are made to the configuration of the virtual machine, the configuration will reapply automatically.                         | <input type="radio"/>            | <input checked="" type="radio"/> |
| If the Web-Server Windows feature is uninstalled from the virtual machine, the discrepancy will be reported in a log entry within 60 minutes. | <input checked="" type="radio"/> | <input type="radio"/>            |

#### Explanation:

No "Dependson" are defined"

No "Mode is Apply and Monitor"

Yes "ConfigurationModeFreqMin : 60 "

-----  
ConfigurationModeFreqMin : How often, in minutes, the current configuration is checked and applied. This property is ignored if the ConfigurationMode property is set to ApplyOnly.

<https://docs.microsoft.com/en-us/powershell/dsc/managing-nodes/metaconfig?view=dsc-1.1>

<https://docs.microsoft.com/en-us/powershell/dsc/configurations/resource-depends-on?view=dsc-1.1>

#### Question: 403

CertyIQ

DRAG DROP -

You have a web app named App1 that is hosted on multiple servers. App1 uses Application Insights in Azure Monitor.

You need to compare the daily CPU usage from the last week for all servers.

How should you complete the query? To answer, drag the appropriate values to the correct targets. 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.

Select and Place:

### Values

bin(timestamp,1d)

bin(timestamp,1h)

project timechart

render chart

render timechart

### Answer Area

```
...
performanceCounters
| where counter == "% Processor Time"
| where timestamp >= ago{7d}
| summarize avg(value) by cloud_RoleInstance,
| ...
...
```

### Answer:

#### Values

bin(timestamp,1d)

bin(timestamp,1h)

project timechart

render chart

render timechart

#### Answer Area

```
...
performanceCounters
| where counter == "% Processor Time"
| where timestamp >= ago{7d}
| summarize avg(value) by cloud_RoleInstance,
| bin(timestamp,1d)
| render timechart
...
...
```

### Question: 404

CertyIQ

You have an Azure subscription that contains 50 virtual machines.

You plan to manage the configuration of the virtual machines by using Azure Automation State Configuration.

You need to create the Desired State Configuration (DSC) configuration files.

How should you structure the code blocks?

- A. Node > Configuration > Resource
- B. Configuration > Resource > Node
- C. Resource > Configuration > Node
- D. Configuration > Node > Resource

### Answer: D

#### Explanation:

-Configuration

-Node

-Resource

"A configuration script consists of the following parts:

The Configuration block. This is the outermost script block. You define it by using the Configuration keyword and providing a name. In this case, the name of the configuration is MyDscConfiguration.

One or more Node blocks. These define the nodes (computers or VMs) that you are configuring. In the above

configuration, there is one Node block that targets a computer named TEST-PC1. The Node block can accept multiple computer names.

One or more resource blocks. This is where the configuration sets the properties for the resources that it is configuring. In this case, there are two resource blocks, each of which call the WindowsFeature resource."

<https://docs.microsoft.com/en-us/powershell/dsc/configurations/configurations?view=dsc-1.1#configuration-syntax>

## Question: 405

CertyIQ

Your team uses Azure Pipelines to deploy applications.

You need to ensure that when a failure occurs during the build or release process, all the team members are notified by using Microsoft Teams. The solution must minimize development effort.

What should you do?

- A. Install the Azure Boards app for Teams and configure a subscription to receive notifications in a channel.
- B. Use Azure Automation to connect to the Azure DevOps REST API and notify the team members.
- C. Use an Azure function to connect to the Azure DevOps REST API and notify the team members.
- D. **Install the Azure Pipelines app for Teams and configure a subscription to receive notifications in a channel.**

### Answer: D

#### Explanation:

Reference:

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

## Question: 406

CertyIQ

DRAG DROP -

You have an app named App1. You have a Log Analytics workspace named Workspace1 that contains a table named AppEvents. App1 writes logs to Workspace1.

You need to query the AppEvents table. The solution must meet the following requirements:

- ⇒ Only query rows for a column named Name that starts with the following text: "Clicked Create New Ticket."
- ⇒ Calculate the number of daily clicks per user.
- ⇒ Return the top 10 users based on their number of clicks for any day.
- ⇒ Sort the results based on the highest number of clicks.
- ⇒ Ignore any users who have less than three daily clicks.

In which order should you arrange the query statements? To answer, move all statements from the list of statements to the answer area and arrange them in the correct order.

Select and Place:

Actions Commands Cmdlets Statements

Answer Area

| summarize NumberOfClicks = count() by bin(TimeGenerated, 1d),  
UserId



AppEvents

| top 10 by NumberOfClicks desc

| where NumberOfClicks >= 3

| where Name startswith "Clicked Create New Ticket"



**Answer:****Actions Commands Cmdlets Statements**

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**Answer Area**

AppEvents

| where Name startswith "Clicked Create New Ticket"

| summarize NumberOfClicks = count() by bin(TimeGenerated, Id),  
UserId

| where NumberOfClicks &gt;= 3

| top 10 by NumberOfClicks desc

**Question: 407****CertyIQ**

HOTSPOT

-

You have an Azure subscription that contains two resource groups named ContosoRG and ContosoDev, an Azure data factory named Contoso Data Factory, and a release pipeline in Azure Pipelines named Pipeline1.

You plan to deploy Contoso Data Factory to ContosoRG by using Pipeline1.

You add the Azure Resource Manager (ARM) template deployment task shown in the following exhibit.

ARM template deployment (1)View YAML RemoveTask version 3.\* ▼Display name \*

Deploy the Contoso Data Factory

Azure Details ^Deployment scope \* (1)

Resource Group

Azure Resource Manager connection \* (1) | Manage (2)

Microsoft Azure Sponsorship

(1) Scoped to subscription 'Microsoft Azure Sponsorship'Subscription \* (1)

Microsoft Azure Sponsorship

Action \* (1)

Create or update resource group

Resource group \* (1)

ContosoRG

Location \* (1)

East US

Template ^Template location \*

Linked artifact

Template \* (1)

\$(System.DefaultWorkingDirectory)/\_Contoso-DataFactory-CI

Template parameters (1)Override template parameters (1)Deployment mode \* (1)

Complete

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 [answer choice] setting must be changed to prevent the modification of existing databases and web apps in ContosoRG.

Action  
Template location  
Deployment mode  
Deployment scope

Pipeline1 will retrieve the ARM template from the [answer choice].

output of the continuous integration build  
location specified in the Linked artifact variable  
default branch of the Git repository of Contoso Data Factory

### Answer:

The [answer choice] setting must be changed to prevent the modification of existing databases and web apps in ContosoRG.

Action  
Template location  
**Deployment mode**  
Deployment scope

Pipeline1 will retrieve the ARM template from the [answer choice].

output of the continuous integration build  
**location specified in the Linked artifact variable**  
default branch of the Git repository of Contoso Data Factory

### Question: 408

CertyIQ

DRAG DROP

You have an Azure Pipeline.

You need to store configuration values as variables.

At which four scopes can the variables be defined, and what is the precedence of the variables from the highest precedence to lowest precedence? To answer, move the appropriate scope from the list of scopes to the answer area and arrange them in the correct order.

#### Scopes

stage

job

pipeline settings UI

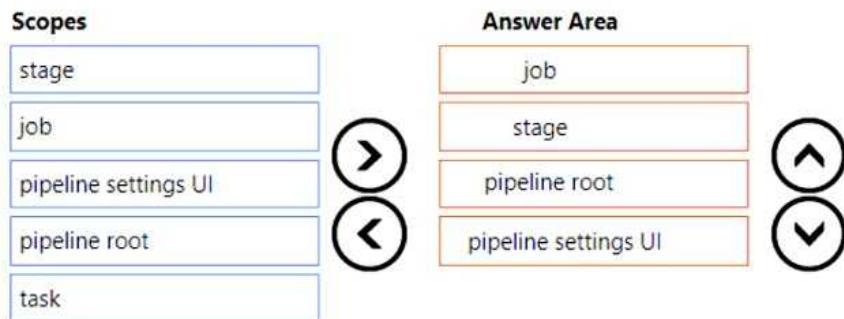
pipeline root

task

#### Answer Area



### Answer:



### Explanation:

When you set a variable with the same name in multiple scopes, the following precedence applies (highest precedence first).

Job level variable set in the YAML file

Stage level variable set in the YAML file

Pipeline level variable set in the YAML file

Variable set at queue time

Pipeline variable set in Pipeline settings UI

<https://learn.microsoft.com/en-us/azure/devops/pipelines/process/variables?view=azure-devops&tabs=yaml%2Cbatch>

### Question: 409

CertyIQ

You have a project in Azure DevOps named Project1 that contains two environments named environment1 and environment2.

When a new version of Project is released, the latest version is deployed to environment2, and the previous version is redeployed to environment1.

You need to distribute users across the environments. The solution must meet the following requirements:

- New releases must be available to only a subset of the users.
- You must gradually increase the number of users that can access environment2.

What should you use?

- VIP swaping
- web app deployment slots
- Azure Load Balancer
- Azure Traffic Manager

Answer: B

**Question: 410**

CertyIQ

DRAG DROP

You are designing a versioning strategy for Git-based packages.

You plan to use a Semantic Versioning (SemVer)-based strategy.

You need to identify when to change the build version.

What should you identify for each scenario? To answer, drag the appropriate versions to the correct scenarios. Each version 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****Answer Area****Major**

You rename a parameter in an API:

**Minor**

You deprecate functionality in an API:

**Patch**

You add a feature and maintain backwards compatibility:

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

You rename a parameter in an API:

**Major**

You deprecate functionality in an API:

**Minor**

You add a feature and maintain backwards compatibility:

**Minor****Question: 411**

CertyIQ

You use Calendar Versioning (CalVer) for code assets.

You need to store an optional tag of beta as part of the version.

Which part of the version should you use for the tag?

- A. minor
- B. major
- C. micro
- D. modifier

**Answer: D**

**Explanation:**

"Major - The first number in the version. 2 and 3 are Python's famous major versions. The major segment is the most common calendar-based component.

Minor - The second number in the version. 7 is the most popular minor version of Python.

Micro - The third and usually final number in the version. Sometimes referred to as the "patch" segment.

Modifier - An optional text tag, such as "dev", "alpha", "beta", "rc1", and so on."

from

<https://calver.org/>

**Question: 412**

CertyIQ

DRAG DROP

You have an Azure subscription that uses Azure Automation State Configuration to manage the configuration of virtual machines.

You need to identify which nodes are noncompliant.

How should you complete the query? To answer, drag the appropriate values to the correct targets. 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**

|                 |                                               |
|-----------------|-----------------------------------------------|
| Category        | AzureDiagnostics                              |
| DscReportStatus | where <input type="text"/> == "DscNodeStatus" |
| Message         | where <input type="text"/> contains ""        |
| OperationName   | where <input type="text"/> != "Compliant"     |
| Resource        |                                               |
| ResultType      |                                               |

**Answer:**

## Answer Area

AzureDiagnostics

```
| where Category == "DscNodeStatus"
| where OperationName contains ""
| where ResultType != "Compliant"
```

### Question: 413

CertyIQ

You have a project in Azure DevOps named Project1.

You need to ensure that all new pipelines in Project1 execute three specific tasks during pipeline execution.

What should you create?

- A. a task group
- B. a JSON template
- C. a YAML template
- D. a PowerShell task

Answer: A

### Question: 414

CertyIQ

HOTSPOT -

You have a project in Azure DevOps that contains a release pipeline. The pipeline contains two stages named QA and Prod. QA deploys code to an Azure web app named webapp1. Prod deploys code to an Azure web app named webapp2.

You need to ensure that code deployments to webapp2 are blocked if Azure Application Insights generates Failed requests alerts following the deployment of new code to webapp1.

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

NOTE: Each correct selection is worth one point.

## Answer Area

QA:

- Add a task to configure alert rules in Application Insights.
- Configure a gate in the pre-deployment conditions.
- Configure an auto-redeploy trigger in the post-deployment conditions
- Configure a post-deployment approval in the post-deployment conditions

Prod:

- Add a task to configure an alert rule in Application Insights.
- Configure a gate in the pre-deployment conditions.
- Configure a trigger in the pre-deployment conditions.
- Configure the Deployment queue settings in the pre-deployment conditions.

Answer:

## Answer Area

QA:

- Add a task to configure alert rules in Application Insights.**
- Configure a gate in the pre-deployment conditions.
- Configure an auto-redeploy trigger in the post-deployment conditions
- Configure a post-deployment approval in the post-deployment conditions

Prod:

- Add a task to configure an alert rule in Application Insights.**
- Configure a gate in the pre-deployment conditions.**
- Configure a trigger in the pre-deployment conditions.
- Configure the Deployment queue settings in the pre-deployment conditions.

### Explanation:

"search for and select Azure App Service deployment with continuous monitoring, and then select Apply."

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

### Question: 415

CertyIQ

You use Azure DevOps processes to build and deploy code.

You need to compare how much time is spent troubleshooting issues found during development and how much time is spent troubleshooting issues found in released code.

Which KPI should you use?

- A. defect escape rate
- B. unplanned work rate

- C. defect rate
- D. rework rate

**Answer: A**

**Explanation:**

The defect escape rate is a metric that assesses the collective quality of software releases by evaluating how often errors are discovered and rectified in the pre-production process versus during production.

### Question: 416

CertyIQ

You have a project in Azure DevOps named Project1.

You implement a Continuous Integration/Continuous Deployment (CI/CD) pipeline that uses PowerShell Desired State Configuration (DSC) to configure the application infrastructure.

You need to perform a unit test and an integration test of the configuration before Project1 is deployed.

What should you use?

- A. the PSScriptAnalyzer tool
- B. the Pester test framework**
- C. the PSCodeHealth module
- D. the Test-DscConfiguration cmdlet

**Answer: B**

**Explanation:**

Use Pester to test a Desired State Configuration to ensure that servers are configured exactly the way you want them: <https://petri.com/testing-dsc-configurations-using-pester/>

### Question: 417

CertyIQ

You use Azure Repos to manage source code and Azure Pipelines to implement continuous integration and continuous deployment (CI/CD).

You need to ensure that all comments on pull requests are resolved before the pull requests are included in a build. The solution must minimize administrative effort.

What should you include in the solution?

- A.a custom action
- B.a post-deployment gate
- C.a branch policy**
- D.a pre-deployment gate

**Answer: C**

**Explanation:**

The correct answer is C

<https://learn.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&tabs=browser#check-for-comment-resolution>

The Check for comment resolution policy checks whether all PR comments are resolved.

### Question: 418

CertyIQ

DRAG DROP

You have a project in Azure DevOps named Project that has a release pipeline in Azure Pipeline named ReleaseP1.

You need to ensure that when a new release is generated for ReleaseP1, a new release note document is created. The release notes must contain new features and bug fixes.

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.

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

| Actions                                                                                  |
|------------------------------------------------------------------------------------------|
| Create a personal access token (PAT).                                                    |
| Create a service principal.                                                              |
| Create a PowerShell task in ReleaseP1 that writes the retrieved data to a markdown file. |
| Create a query that retrieves the feature and bug fix information.                       |
| Add a dashboard widget that retrieves the feature and bug fix information.               |

Answer Area

|   |
|---|
| 1 |
| 2 |
| 3 |



### Answer:

| Actions                                                                                  |
|------------------------------------------------------------------------------------------|
| Create a personal access token (PAT).                                                    |
| Create a service principal.                                                              |
| Create a PowerShell task in ReleaseP1 that writes the retrieved data to a markdown file. |
| Create a query that retrieves the feature and bug fix information.                       |
| Add a dashboard widget that retrieves the feature and bug fix information.               |

| Answer Area                                                                                |
|--------------------------------------------------------------------------------------------|
| 1 Create a query that retrieves the feature and bug fix information.                       |
| 2 Create a personal access token (PAT).                                                    |
| 3 Create a PowerShell task in ReleaseP1 that writes the retrieved data to a markdown file. |

### Explanation:

1. Create Query that retrieves the feature and bux fix information
2. Create PAT
3. Create Powershell task in ReleaseP1 that writes the retived data to a markdown file.

<https://slothycode.com/azure-pipelines-publish-release-notes/>

### Question: 419

CertyIQ

HOTSPOT -

You need to configure the alert for VM1. The solution must meet the technical requirements.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Alert logic

|             |              |                      |         |                     |   |
|-------------|--------------|----------------------|---------|---------------------|---|
| Threshold ⓘ | Static       | Dynamic              |         |                     |   |
| Operator ⓘ  | Greater than | Aggregation type * ⓘ | Average | Threshold value * ⓘ | % |

### Condition preview

Whenever the average percentage cpu is greater than <logic undefined> %

### Evaluated based on

|                                      |           |                           |                |
|--------------------------------------|-----------|---------------------------|----------------|
| Aggregation granularity (Period) * ⓘ | 5 minutes | Frequency of evaluation ⓘ | Every 1 Minute |
|--------------------------------------|-----------|---------------------------|----------------|

## Answer:

### Alert logic

|             |              |                      |         |                     |   |
|-------------|--------------|----------------------|---------|---------------------|---|
| Threshold ⓘ | Static       | Dynamic              |         |                     |   |
| Operator ⓘ  | Greater than | Aggregation type * ⓘ | Average | Threshold value * ⓘ | % |

### Condition preview

Whenever the average percentage cpu is greater than <logic undefined> %

### Evaluated based on

|                                      |           |                           |                |
|--------------------------------------|-----------|---------------------------|----------------|
| Aggregation granularity (Period) * ⓘ | 5 minutes | Frequency of evaluation ⓘ | Every 1 Minute |
|--------------------------------------|-----------|---------------------------|----------------|

## Explanation:

Setting 1: Threshold value -

Set to 80 %

Scenario: An Azure Monitor alert for VM1 must be configured to meet the following requirements:

- ⇒ Be triggered when average CPU usage exceeds 80 percent for 15 minutes.
- ⇒ Calculate CPU usage averages once every minute.

Setting 2: Aggregation granularity

Set to 15 minutes.

## Question: 420

CertyIQ

DRAG DROP -

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

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

Select and Place:

## Actions

## Answer Area

Create a fork

Create a branch

Add a build validation policy.



Add a build policy



Create a repository

Add an application access policy.

### Answer:

#### Actions                          Answer Area

Create a fork

Create a fork

Create a branch

Add a build validation policy.



Add a build policy



Add an application access policy.

### Explanation:

Step 1: Create a Fork

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.**

### Question: 421

CertyIQ

You have an Azure subscription that contains the resources shown in the following table.

| Name         | Type                             |
|--------------|----------------------------------|
| DepPipeline1 | Azure DevOps deployment pipeline |
| ADFPipeline1 | Azure Data Factory pipeline      |
| Vault1       | Azure Key Vault                  |

DepPipeline1 and ADFPipeline1 use a single credential that is stored in Vault1.

You need to configure ADFPipeline1 to retrieve the credential from Vault1.

Which type of activity should you use?

- A.Lookup
- B.Get Metadata
- C.Copy
- D.Web

### Answer: D

#### Explanation:

D is the answer.

<https://learn.microsoft.com/en-us/azure/data-factory/how-to-use-azure-key-vault-secrets-pipeline-activities#stepsIn> your Data Factory pipeline, add a new Web activity and configure it as follows.

### Question: 422

CertyIQ

DRAG DROP -

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

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

Select and Place:

| Actions                                   | Answer Area |
|-------------------------------------------|-------------|
| 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:**

| Actions                                   | Answer Area |
|-------------------------------------------|-------------|
| 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.                            |             |

**Explanation:**

It was clearly mentioned New code/repo should be a copy of project2 - so when you create a new repo you will not get the copy of existing code to make a new experiment on some part of code.

step 1: You will fork - Now you got the copy of project2

step2: Add the build policy - unfortunately after you fork you will not get the policies inherit, also you already got the project2 branching here( no need to create a master branch or so)

step3: create a branch - now you create a branch to make your own changes and you will test the code functionality -if everything is good you will submit the code ( here pull request is managed by main project 2 team)

**Question: 423**

You have an Azure web app that is deployed by using Azure Pipelines.

CertyIQ

You need to ensure that when a new version of the app is deployed to production, you can roll back to the previous version. The solution must meet the following requirements:

- Minimize downtime during the deployment.
- Minimize the time it takes for the rollback.

What should you use?

- A.a single web app and two deployment slots
- B.a single web app and two deployment pipelines
- C.two web apps and an Azure Standard Load Balancer
- D.two web apps and an Azure Traffic Manager instance

**Answer: A**

**Explanation:**

A: a single web app and two deployment slots

#### Question: 424

CertyIQ

You have an app named App1 that you release by using Azure Pipelines. App1 has the versions shown in the following table.

| Number | Description      |
|--------|------------------|
| 3.4.7  | Previous release |
| 4.0.0  | Current release  |

You complete a code change to fix a bug that was introduced in version 3.4.3.

Which version number should you assign to the release?

- A.3.4.4
- B.3.4.8
- C.3.5.0
- D.4.0.1

**Answer: D**

**Explanation:**

Based on the given information, the current release of App1 is version 4.0.0, and you have made a code change to fix a bug that was introduced in version 3.4.3. Following semantic versioning principles, the bug fix should be considered a patch, as it does not introduce any new features or breaking changes. Therefore, the version number for the release should be incremented in the patch position. Since the current release is 4.0.0, the next appropriate version number for the bug fix release would be 4.0.1.

#### Question: 425

CertyIQ

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.Playwright**
- C.Xamarin.UITest
- D.Microsoft.CodeAnalysis

**Answer: B**

**Explanation:**

Correct Answer : B Playwright - Playwright is a cross-browser automation library developed by Microsoft. It supports multiple programming languages, including JavaScript, Python, and .NET. Playwright allows you to automate interactions with web pages in various browsers, including Chrome, Firefox, and Safari. It offers features like parallel test execution, robust element selectors, and built-in support for modern web technologies.

### Question: 426

CertyIQ

You have a project in Azure DevOps named Project1 that references an Azure Artifacts feed named Feed1.

You have a package named Package1 that has the versions shown in the following table.

| Version | Description                       |
|---------|-----------------------------------|
| 1.0.3   | Manually pushed to Feed1          |
| 1.4.0   | Manually pushed to Feed1          |
| 2.0.0   | Available from an upstream source |
| 2.3.1   | Saved from an upstream source     |

You need to perform a build of Project1.

Which version of Package1 will be used?

- A.1.0.3
- B.1.4.0
- C.2.0.0
- D.2.3.1**

**Answer: D**

**Explanation:**

Correct D. 2.3.1

### Question: 427

CertyIQ

HOTSPOT

-

You have an Azure subscription.

You need to create a storage account by using a Bicep file.

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

NOTE: Each correct selection is worth one point.

#### Answer Area

```
param storageAccount string

var storageAccountNameToUse = '${storageAccount}${uniqueString(resourceGroup().id)}'

resource invoiceStorage 'Microsoft.Storage/storageAccounts@2022-05-01' = {
 name: storageAccountNameToUse
 location: 'eastus'
 sku: {
 name: 'Standard_GRS'
 }
 kind: 'StorageV2'
 param: {
 properties: {
 type: 'Standard_LRS'
 }
 }
 properties: {
 supportsHttpsTrafficOnly: true
 }
}
```

**Answer:**

## Answer Area

```
param storageAccount string

var storageAccountNameToUse = '${storageAccount}${uniqueString(resourceGroup().id)}'

resource invoiceStorage 'Microsoft.Storage/storageAccounts@2022-05-01' = {
 name: storageAccountNameToUse
 location: 'eastus'
 sku: {
 name: 'Standard_GRS'
 }
}

kind: 'StorageV2'
param:
properties:
type:
var:

{
 kind:
 param:
 properties:
 type:
 var:
 supportsHttpsTrafficOnly: true
 }
}
```

### Explanation:

1. kind
2. properties

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/resource-declaration?tabs=azure-powershell#resource-specific-properties>

## Question: 428

CertyIQ

DRAG DROP -

You are configuring the Azure DevOps dashboard. The solution must meet the technical requirements. Which widget should you use for each metric? To answer, drag the appropriate widgets to the correct metrics. Each 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.

Select and Place:

## Widgets

## Metrics

Velocity

Query tile

Query results

Sprint burndown

Cumulative flow diagram

Release pipeline overview

1:

2:

3:

Answer:

## Widgets

## Metrics

Velocity

Query tile

Query results

Sprint burndown

Cumulative flow diagram

Release pipeline overview

1: Sprint burndown

2: Release pipeline overview

3: Query tile

### Explanation:

Box 1: Sprint burndown

Box 2: Release pipeline overview

Release pipeline overview shows the status of environments in a release definition.

### Box 3: Query tile -

Query tile displays the total number of results from a query.

<https://docs.microsoft.com/en-us/azure/devops/report/dashboards/team-velocity?view=azure-devops>

CertyIQ

### Question: 429

You plan to deploy a new database environment. The solution must meet the technical requirements.

You need to prepare the database for the deployment.

How should you format the export?

- A.NDF
- B.BACPAC**
- C.DACPAC
- D.MDF

### Answer: B

#### Explanation:

The initial databases for new environments must contain both schema and reference data.

When you need to export a database for archiving or for moving to another platform, you can export the database schema and data to a BACPAC file. A BACPAC file is a ZIP file with an extension of BACPAC containing the metadata and data from the database. A BACPAC file can be stored in Azure Blob storage or in local storage in an on-premises location and later imported back into Azure SQL Database, Azure SQL Managed Instance, or a SQL Server instance.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/database-export>

CertyIQ

### Question: 430

You need to meet the technical requirements for monitoring App1.

What should you use?

- A.Splunk
- B.Azure Application Insights**
- C.Azure Advisor
- D.App Service logs

### Answer: B

#### Explanation:

B (Page load times = Azure Application Insights)

CertyIQ

### Question: 431

HOTSPOT -

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

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:

## Answer Area

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   |

@

### **Explanation:**

Scenario:

**Project5 will contain a Git repository in Azure Reports and a continuous integration trigger that will initiate a build in response to any change except for changes within /folder1 of the repository.**

Continuous integration (CI) triggers cause a build to run whenever a push is made to the specified branches or a specified tag is pushed.

Box 2: branch filter to include -

You can specify branches to include and exclude. For example:

# specific branch build

trigger:

branches:

include:

- master

- releases/\*

exclude:

- releases/old\*

References:

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

**CertyIQ**

### **Question: 432**

In Azure DevOps, you create Project3.

You need to meet the requirements of the project.

What should you do first?

- A.From Azure DevOps, modify the build definition.
- B.From SonarQube, obtain an authentication token.**
- C.From Azure DevOps, create a service endpoint.
- D.From SonarQube, create a project.

### **Answer: B**

### **Explanation:**

B is the answer

<https://learn.microsoft.com/en-us/azure/devops/pipelines/tasks/reference/sonar-qube-prepare-v5?view=azure-pipelines>Specifies the SonarQube server endpoint for your project. To create one, click the Manage link, create a new SonarQube Server Endpoint, and enter your server url and token.

The Azure devops service connection asks for sonar qube token to register it. So Answer should be B.

**Question: 433**

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. |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|           |                                                                                                                                                                                |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.

**Reference:**

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

**Question: 434****DRAG DROP -**

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.

Select and Place:

**Actions****Answer Area**

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:**

| Actions                                                                                         | Answer Area                                                                                                      |
|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
|                                                                                                 | 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. |                                                                                                                  |

**Explanation:**

Scenario:

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

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

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

Step 2: Create a personal access token..

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

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

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

Reference:

<https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-tutorial-deploy-container-app-with-ci-cd-vsts> <https://mohitgoyal.co/2019/01/10/run-azure-devops-private-agents-in-kubernetes-clusters/>  
[Implement Continuous Integration](#)

**Question: 435****CertyIQ**

You add the virtual machines as managed nodes in Azure Automation State Configuration.

You need to configure the managed computers in Pool7.

What should you do next?

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

**Answer: B**

### Explanation:

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

Scenario: The Azure DevOps organization includes:

The Docker extension -

A deployment pool named Pool7 that contains 10 Azure virtual machines that run Windows Server 2019

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode>

### Question: 436

CertyIQ

DRAG DROP -

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

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

Select and Place:

#### Actions

Create a fork

Create a branch

Add a build policy for the fork

Add a build policy for the master branch

Create a repository

Add an application access policy.

#### Answer Area



Answer:

## Actions

Create a fork

Create a branch

Add a build policy for the fork

Add a build policy for the master branch

Create a repository

Add an application access policy.

## Answer Area

Create a fork

Add a build policy for the master branch

Add an application access policy.



### Explanation:

Create a fork- Add a build policy for the master branch- Add an application access policy.

<https://docs.microsoft.com/en-us/azure/devops/repos/git/forks?view=azure-devops&tabs=visual-studio#whats-in-a-fork>

## Question: 437

CertyIQ

DRAG DROP -

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.

Select and Place:

### Actions

### Answer Area

Run the `Import-AzureRmAutomationDscConfiguration` Azure PowerShell cmdlet.

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

Run the `New-AzureRmResourceGroupDeployment` Azure PowerShell cmdlet.

Run the `Start-AzureRmAutomationDscCompilationJob` 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.                                                                                                                                    |
| Create a Desired State Configuration (DSC) configuration file that has an extension of .ps1. | Run the <code>Import-AzureRmAutomationDscConfiguration</code> Azure PowerShell cmdlet.                                                                                                                                          |
| Run the <code>New-AzureRmResourceGroupDeployment</code> Azure PowerShell cmdlet.             | <input checked="" type="radio"/> Run the <code>Start-AzureRmAutomationDscCompilationJob</code> Azure PowerShell cmdlet.<br><input type="radio"/> Create an Azure Resource Manager template file that has an extension of .json. |
| Run the <code>Start-AzureRmAutomationDscCompilationJob</code> Azure PowerShell cmdlet.       |                                                                                                                                                                                                                                 |
| Create an Azure Resource Manager template file that has an extension of .json.               |                                                                                                                                                                                                                                 |

### Explanation:

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

Step 2: Run the `Import-AzureRmAutomationDscConfiguration` Azure Powershell cmdlet

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

Example:

```
PS C:\>Import-AzureRmAutomationDscConfiguration -AutomationAccountName "Contoso17" -ResourceGroupName "ResourceGroup01" -SourcePath "C:\DSC\client.ps1" -Force
```

This command imports the DSC configuration in the file named client.ps1 into the Automation account named Contoso17. The command specifies the Force parameter. If there is an existing DSC configuration, this command replaces it.

Step 3: Run the `Start-AzureRmAutomationDscCompilationJob` Azure Powershell cmdlet

The `Start-AzureRmAutomationDscCompilationJob` cmdlet compiles an APS Desired State Configuration (DSC) configuration in Azure Automation.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/import-azurermautomationdscconfiguration> <https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/start-azurermautomationdsccompilationjob>

### Question: 438

CertyIQ

HOTSPOT -

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.

Hot Area:

## Answer Area

Required secrets:

|                                   |
|-----------------------------------|
| Certificate                       |
| Personal access token             |
| Shared Access Authorization token |
| Username and password             |

Storage location:

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

Answer:

## Answer Area

Required secrets:

|                                   |
|-----------------------------------|
| Certificate                       |
| Personal access token             |
| Shared Access Authorization token |
| Username and password             |

Storage location:

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

### Explanation:

Box 1: Shared Access Authorization token

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

#### Box 2: Azure Storage with HTTPS access

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

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

Reference:

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

### Question: 439

CertyIQ

HOTSPOT -

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

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:

## Answer Area

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:

1. Username and Password
2. Azure Key vault

## Question: 440

CertyIQ

DRAG DROP -

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.

Select and Place:

### Access Levels

Collaborator

Contributor

Owner

Reader

### Answer Area

Developers:

Team Leaders:

**Answer:**

### Access Levels

Collaborator

Contributor

Owner

Reader

### Answer Area

Developers:

Reader

Team Leaders:

Owner

### Explanation:

Box 1: Reader -

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

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

Box 2: Owner -

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

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

### Question: 441

You need to meet the technical requirements for controlling access to Azure DevOps.  
What should you use?

CertyIQ

- A.Azure Multi-Factor Authentication (MFA)
- B.on-premises firewall rules
- C.conditional access policies in Azure AD**
- D.Azure role-based access control (Azure RBAC)

**Answer: C**

**Explanation:**

Scenario: Access to Azure DevOps must be restricted to specific IP addresses.

Azure DevOps is authenticated through Azure Active Directory. You can use Azure AD's conditional access to prevent logins from certain geographies and address ranges.

Reference:

<https://www.rebeladmin.com/2018/08/step-step-guide-configure-location-based-conditional-access-policies/>

### Question: 442

**CertyIQ**

You need to configure Azure Pipelines to control App2 builds.  
Which authentication method should you use?

- A.Windows NTLM
- B.certificate
- C.SAML
- D.personal access token (PAT)**

**Answer: D**

**Explanation:**

Scenario: Deploy App2 to an Azure virtual machine named VM1.

A personal access token (PAT) is used as an alternate password to authenticate into Azure DevOps.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/use-personal-access-tokens-to-authenticate>

### Question: 443

**CertyIQ**

DRAG DROP -

You need to configure authentication for App1. The solution must support the planned changes.  
Which three actions should you perform in sequence? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

## Actions Commands Cmdlets Statements

## Answer Area

Create an app.

Add a secret.

Create a credential.

Configure the ID and secret for App1.

Create a managed service identity.



Answer:

## Actions Commands Cmdlets Statements

## Answer Area

Create an app.

Add a secret.

Configure the ID and secret for App1.

Add a secret.

Create a credential.



### Explanation:

1) Create app  
2) Add secret  
3) Configure ID and secret

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>  
After you add a secret you have to configure it for the app right.

## Question: 444

CertyIQ

Your company builds a multi-tier web application.

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

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

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

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

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

**Answer: D**

**Explanation:**

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

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

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

Reference:

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

**Question: 445**

**CertyIQ**

DRAG DROP -

You need to recommend a solution for deploying charts by using Helm and Tiller to Azure Kubernetes Service (AKS) in an RBAC-enabled cluster.

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

Select and Place:

**Answer:**

**Commands**

**Answer Area**

helm completion

kubectl create

helm init

helm install

helm serve



Explanation

## Explanation:

### Step 1: Kubectl create -

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

Example: Service account with cluster-admin role

```
$ kubectl create -f rbac-config.yaml
```

```
serviceaccount "tiller" created
```

```
clusterrolebinding "tiller" created
```

```
$ helm init --service-account tiller
```

### Step 2: helm init -

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

### Step 3: helm install -

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

References:

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

[https://docs.helm.sh/using\\_helm/#tiller-namespaces-and-rbac](https://docs.helm.sh/using_helm/#tiller-namespaces-and-rbac)

CertyIQ

## Question: 446

DRAG DROP -

You need to configure access to Azure DevOps agent pools to meet the following requirements:

- ⇒ Use a project agent pool when authoring build or 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 memberships 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 view content.

NOTE: Each correct selection is worth one point.

Select and Place:

## Answer:

**Roles****Answer Area**

Administrator

Reader

Service Account

User

Organization:

Reader

Project:

User

**Explanation****Explanation:**

Box 1: Reader -

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

Box 2: User

Service Account is a role on organization level for creating a project agent pool in a project. User role is a role on project level for using the project agent pool when authoring pipeline.

**Question: 447****CertyIQ****HOTSPOT -**

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.

Hot Area:

**Answer:**

## Answer Area

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

### Explanation:

#### Box 1: Microsoft Visual Studio App Center distribution Groups

Distribution Groups are used to control access to releases. A Distribution Group represents a set of users that can be managed jointly and can have common access to releases. 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>

## Question: 448

CertyIQ

DRAG DROP -

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.

Select and Place:

### Answer:

## Build Agent Pools

## Answer Area

- Hosted Windows Container
- Hosted Linux
- Hosted macOS
- Hosted
- Default

An application that runs on iOS:

Hosted

An Internet Information Services (IIS) web application that runs in Docker:

Hosted

### Explanation

#### Explanation:

Box 1: Hosted

Box 2: Hosted -

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

### Incorrect Answers:

Default pool: Use it to register self-hosted agents that you've set up.

Hosted Windows Container pool (Azure Pipelines only): Enabled you to build and release inside Windows containers. Unless you're building using containers,

Windows builds should run in the Hosted VS2017 or Hosted pools.

## Question: 449

CertyIQ

DRAG DROP -

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

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

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

Select and Place:

### Answer:

## Actions

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 Area

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.

## Explanation

### Explanation:

Step 1: Assign the node configuration.

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

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

You import the configuration into the Automation account.

Step 3: Compiling a configuration into a node configuration

Compiling a configuration in Azure Automation

Before you can apply a desired state to a node, a DSC configuration defining that state must be compiled into one or more node configurations (MOF document), and placed on the Automation DSC Pull Server.

Step 4: Onboard the virtual machines to Azure State Configuration

Onboarding an Azure VM for management with Azure Automation State Configuration

Step 5: Check the compliance status of the node.

Viewing reports for managed nodes. Each time Azure Automation State Configuration performs a consistency check on a managed node, the node sends a status report back to the pull server. You can view these reports on the page for that node.

On the blade for an individual report, you can see the following status information for the corresponding consistency check:

The report status "" whether the node is "Compliant", the configuration "Failed", or the node is "Not Compliant" (when the node is in ApplyandMonitor mode and the machine is not in the desired state).

References:

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

CertyIQ

### Question: 450

HOTSPOT -

You have a project in 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.

Hot Area:

Answer:

#### Answer Area

```
"resources": [
 {
 "apiVersion": "2018-05-01",
 "name": "secrets",
 "type": "Microsoft.KeyVault/vaults",
 "Microsoft.Resources/deployments",
 "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

#### Explanation:

Box 1: "Microsoft.Resources/deployments"

Reference a secret with dynamic ID. You need to reference a key vault secret that varies based on the current deployment.

Example:

```
"resources": [
 "apiVersion": "2018-05-01",
 "name": "dynamicSecret",
 "type": "Microsoft.Resources/deployments",
 "properties":
 "mode": "Incremental",
 "templateLink":
 Box 2: "templateLink"
```

In your parent template, you add the linked template and pass in a parameter that contains the dynamically generated resource ID.

References:

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

## Question: 451

CertyIQ

DRAG DROP -

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.

Select and Place:

Answer:

**Components**

**Answer Area**

A deployment group

Ten virtual machines hosted in Azure:

A deployment group

A management group

Ten virtual machines hosted in  
an on-premises data center environment:

A deployment group

A resource group

Application roles

## Explanation

### Explanation:

Box 1: A deployment group -

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

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

Box 2: A deployment group -

References:

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

CertyIQ

## Question: 452

DRAG DROP -

You have an Azure Kubernetes Service (AKS) implementation that is RBAC-enabled.

You plan to use Azure Container Instances as a hosted development environment to run containers in the AKS implementation.

You need to configure Azure Container Instances as a hosted environment for running the containers in AKS. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

### Answer:

#### Actions

Run helm init.

Run az aks install-connector.

Create a YAML file.

Run az role assignment create

Run kubectl apply.

#### Answer Area

Run kubectl apply.

Run helm init.

Run az aks install-connector.



## Explanation

### Explanation:

1. kubectl apply - to create the service principle for Tiller2.
2. helm init - to deploy Tiller in the kubernetes cluster
3. az aks install-connector - to install the connector

**HOTSPOT -**

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.

Hot Area:

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

Developers:

|             |
|-------------|
| Basic       |
| Stakeholder |

Pilot users:

|             |
|-------------|
| Basic       |
| Stakeholder |

Explanation

**Explanation:**

Box 1: Basic -

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

Box 2: Stakeholder -

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

Note:

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

Basic: provides access to most features

VS Enterprise: provides access to premium features

Stakeholders: provides partial access, can be assigned to unlimited users for free

References:

**Question: 454**

HOTSPOT -

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer:**

## Answer Area

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](#)

### Explanation:

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

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

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

### References:

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

HOTSPOT -

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.

Hot Area:

Answer:

## Answer Area

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.

Explanation

### Explanation:

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

Box 1: Set the default retention policy to 30 days

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

Box 2: Set the stage retention policy to 60 days

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

References:

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

## HOTSPOT -

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.

Hot Area:

**Answer:**

## Answer Area

Developers:

|             |
|-------------|
| Basic       |
| Stakeholder |

Pilot users:

|             |
|-------------|
| Basic       |
| Stakeholder |

Explanation

### Explanation:

Box 1: Basic -

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

Box 2: Stakeholder -

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

Note:

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

Basic: provides access to most features

VS Enterprise: provides access to premium features

Stakeholders: provides partial access, can be assigned to unlimited users for free

References:

<https://docs.microsoft.com/en-us/azure/devops/organizations/security/access-levels?view=vsts>

## Question: 457

CertyIQ

DRAG DROP -

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.

Select and Place:

**Answer:**

**Components**

**Answer Area**

A deployment group

Ten virtual machines hosted in Azure:

A deployment group

A management group

Ten virtual machines hosted in  
an on-premises data center environment:

A deployment group

A resource group

Application roles

Explanation

**Explanation:**

Box 1: A deployment group -

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

If the target machines are Azure VMs, you can quickly and easily prepare them by installing the Azure

Pipelines Agent Azure VM extension on each of the VMs, or by using the Azure Resource Group Deployment task in your release pipeline to create a deployment group dynamically.

Box 2: A deployment group -

References:

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

## Question: 458

CertyIQ

DRAG DROP -

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.

Select and Place:

**Answer:**

## Chart Widgets      Answer Area

Burndown

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

Lead Time

Cycle Time

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

Cycle Time

Lead Time

The remaining work:

Burndown

Explanation

### Explanation:

Box 1: Lead time -

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

Box 2: Cycle time -

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

Box 3: Burndown -

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

Incorrect Answers:

- ⇒ Velocity provides a useful metric for these activities:
- ⇒ Support sprint planning
- ⇒ Forecast future sprints and the backlog items that can be completed
- ⇒ A guide for determining how well the team estimates and meets their planned commitments

References:

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

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

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

**Question: 459**

DRAG DROP -

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

**CertyIQ**

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 targets. 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.

Select and Place:

**Answer:**

**Security Tools**

**Answer Area**

Pull request: Static code analysis

Continuous integration: Static code analysis

Continuous delivery: Penetration testing

**Explanation**

**Explanation:**

Box 1: static code analysis

Box 2: Static code analysis -

Validation in the CI/CD begins before the developer commits his or her code. Static code analysis tools in the IDE provide the first line of defense to help ensure that security vulnerabilities are not introduced into the CI/CD process.

Box 3: Penetration testing -

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

**References:**

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

**Question: 460**

CertyIQ

**HOTSPOT -**

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.

Hot Area:

**Answer:**

## Answer Area

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:

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.

## Question: 461

CertyIQ

DRAG DROP -

You need to recommend a solution for deploying charts by using Helm and Tiller to Azure Kubernetes Service (AKS) in an RBAC-enabled cluster.

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

Select and Place:

**Answer:**

## Actions

Run helm init.

Run az aks install-connector.

Create a YAML file.

Run az role assignment create

Run kubectl apply.

### Explanation:

Run kubectl apply

Run helm init

Run az aks install connector

## Answer Area

Run kubectl apply.

Run helm init.

Run az aks install-connector.



## Question: 462

CertyIQ

### DRAG DROP -

You need to configure access to Azure DevOps agent pools to meet the following requirements:

- ⇒ Use a project agent pool when authoring build or 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 memberships 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 view content.

NOTE: Each correct selection is worth one point.

Select and Place:

### Answer:

## Roles

## Answer Area

Administrator

Reader

Service Account

User

Organization:

Reader

Project:

User

### Explanation:

Box 1: Reader -

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

Box 2: user

## Question: 463

CertyIQ

HOTSPOT -

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.

Hot Area:

Answer:

## Answer Area

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:

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>

CertyIQ

### Question: 464

DRAG DROP -

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.

Select and Place:

Answer:

#### Build Agent Pools

#### Answer Area

Hosted Windows Container

An application that runs on iOS:

Hosted

Hosted macOS

An Internet Information Services (IIS) web application that runs in Docker:

Hosted

Hosted

Default

### Explanation:

Box 1: Hosted

Box 2: Hosted -

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

agents.

Incorrect Answers:

Default pool: Use it to register self-hosted agents that you've set up.

Hosted Windows Container pool (Azure Pipelines only): Enabled you to build and release inside Windows containers. Unless you're building using containers,

Windows builds should run in the Hosted VS2017 or Hosted pools.

CertyIQ

### Question: 465

DRAG DROP -

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

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

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

Select and Place:

Answer:

#### Actions

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 Area

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.

Explanation

#### Explanation:

Step 1: Assign the node configuration.

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

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

You import the configuration into the Automation account.

## Step 3: Compiling a configuration into a node configuration

Compiling a configuration in Azure Automation

Before you can apply a desired state to a node, a DSC configuration defining that state must be compiled into one or more node configurations (MOF document), and placed on the Automation DSC Pull Server.

## Step 4: Onboard the virtual machines to Azure State Configuration

Onboarding an Azure VM for management with Azure Automation State Configuration

## Step 5: Check the compliance status of the node.

Viewing reports for managed nodes. Each time Azure Automation State Configuration performs a consistency check on a managed node, the node sends a status report back to the pull server. You can view these reports on the page for that node.

On the blade for an individual report, you can see the following status information for the corresponding consistency check:

The report status "" whether the node is "Compliant", the configuration "Failed", or the node is "Not Compliant" (when the node is in ApplyandMonitor mode and the machine is not in the desired state).

References:

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

CertyIQ

## Question: 466

HOTSPOT -

You have a project in 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.

Hot Area:

## Answer:

## Answer Area

```
"resources": [
 {
 "apiVersion": "2018-05-01",
 "name" : "secrets",
 "type": "Microsoft.Resources/deployments",
 "dependsOn": [
 "Microsoft.KeyVault/vaults",
 "Microsoft.Resources/deployments",
 "Microsoft.Subscription/subscriptions"
],
 "properties": {
 "mode" : "Incremental",
 "templateLink": {
 "deployment": "nestedTemplate"
 }
 },
 "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:

Box 1: "Microsoft.Resources/deployments"

Reference a secret with dynamic ID. You need to reference a key vault secret that varies based on the current deployment.

Example:

```
"resources": [
 {
 "apiVersion": "2018-05-01",
 "name": "dynamicSecret",
 "type": "Microsoft.Resources/deployments",
 "properties": {
 "mode": "Incremental",
 "templateLink": {
 "deployment": "nestedTemplate"
 }
 }
 }
],
```

Box 2: "templateLink"

In your parent template, you add the linked template and pass in a parameter that contains the dynamically generated resource ID.

References:

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

### Question: 467

CertyIQ

DRAG DROP -

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.

Select and Place:

Answer:

Components

Answer Area

A deployment group

Ten virtual machines hosted in Azure:

A deployment group

A management group

Ten virtual machines hosted in  
an on-premises data center environment:

A deployment group

A resource group

Application roles

Explanation:

Box 1: A deployment group -

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

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

Box 2: A deployment group -

References:

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

### Question: 468

CertyIQ

DRAG DROP -

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

**Answer:**

**Actions**

Run helm init.

Run az aks install-connector.

Create a YAML file.

Run az role assignment create

Run kubectl apply.

**Answer Area**

Run kubectl apply.

Run helm init.

Run az aks install-connector.



**Explanation:**

kubectl apply helm init az aks install-connector

**Question: 469**

CertyIQ

**HOTSPOT -**

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.

Hot Area:

**Answer:**

# Answer Area

Developers:

|             |
|-------------|
| Basic       |
| Stakeholder |

Pilot users:

|             |
|-------------|
| Basic       |
| Stakeholder |

## Explanation:

Box 1: Basic -

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

Box 2: Stakeholder -

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

Note:

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

Basic: provides access to most features

VS Enterprise: provides access to premium features

Stakeholders: provides partial access, can be assigned to unlimited users for free

References:

<https://docs.microsoft.com/en-us/azure/devops/organizations/security/access-levels?view=vsts>

## Question: 470

CertyIQ

HOTSPOT -

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer:

## Answer Area

Required secrets:

|                                   |
|-----------------------------------|
| Certificate                       |
| Personal access token             |
| Shared Access Authorization token |
| <b>Username and password</b>      |

Storage location:

|                                 |
|---------------------------------|
| Azure Data Lake                 |
| <b>Azure Key Vault</b>          |
| Azure Storage with HTTP access  |
| Azure Storage with HTTPS access |

### Explanation:

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

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

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

### References:

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

## Question: 471

CertyIQ

HOTSPOT -

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.

Hot Area:

### Answer:

## Answer Area

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.

### Explanation:

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

Box 1: Set the default retention policy to 30 days

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

Box 2: Set the stage retention policy to 60 days

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

### References:

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

### Question: 472

CertyIQ

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>

Implement Application Infrastructure

**CertyIQ****Question: 473**

You have a multi-tier application that has an Azure Web Apps front end and an Azure SQL Database back end. You need to recommend a solution to capture and store telemetry data. The solution must meet the following requirements:

- ⇒ Support using ad-hoc queries to identify baselines.
  - ⇒ Trigger alerts when metrics in the baseline are exceeded.
- Store application and database metrics in a central location.

What should you include in the recommendation?

- A.Azure Event Hubs
- B.Azure SQL Database Intelligent Insights
- C.Azure Application Insights
- D.Azure Log Analytics

**Answer: D****Explanation:**

Azure Platform as a Service (PaaS) resources, like Azure SQL and Web Sites (Web Apps), can emit performance metrics data natively to Log Analytics.

The Premium plan will retain up to 12 months of data, giving you an excellent baseline ability.

There are two options available in the Azure portal for analyzing data stored in Log analytics and for creating queries for ad hoc analysis.

Incorrect Answers:

B: Intelligent Insights analyzes database performance by comparing the database workload from the last hour with the past seven-day baseline workload. However, we need handle application metrics as well.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-azurepass-posh>

**CertyIQ****Question: 474**

DRAG DROP -

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.

Select and Place:

### Answer: Explanation

#### Explanation:

Box 1: A key Vault advanced access policy

The screenshot shows the 'mykeyvault0920 - Access policies' page in the Azure portal. The left sidebar lists 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings' (with 'Keys', 'Secrets', 'Certificates'), 'Access policies' (which is selected and highlighted in blue), and 'Firewalls and virtual networks'. The main pane displays three checkboxes under 'Click to hide advanced access policies': 'Enable access to Azure Virtual Machines for deployment' (unchecked), 'Enable access to Azure Resource Manager for template deployment' (checked), and 'Enable access to Azure Disk Encryption for volume encryption' (unchecked). Below these checkboxes is a 'Add new' button and a row containing a user icon, '<Your username>', and 'USER'. The entire row for the user entry is highlighted with a red box.

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.

Reference:

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

### Question: 475

CertyIQ

DRAG DROP -

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"> <li>Changes must be reviewed by at least two project members.</li> <li>Changes must be associated to at least one work team.</li> </ul> |
| 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.

Select and Place:

#### Answer:

#### Version Control Systems

Git

Perforce

Subversion

Team Foundation Version Control

#### Answer Area

Project 1: Team Foundation Version Control

Project 2: Git

Project 3: Git

Project 4: Team Foundation Version Control

#### Explanation:

Box 1: Team Foundation Version Control

TFVC lets you apply granular permissions and restrict access down to a file level.

Box 2: Git -

Git is the default version control provider for new projects. You should use Git for version control in your projects unless you have a specific need for centralized version control features in TFVC.

Box 3: Git

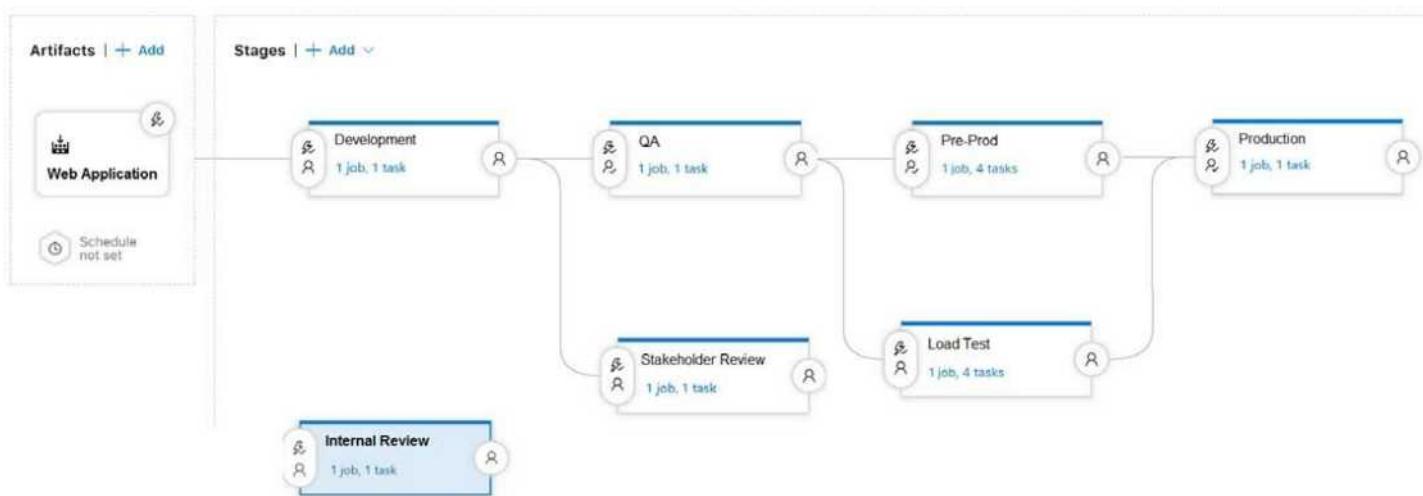
Box 4: Team Foundation Version Control

#### Question: 476

HOTSPOT -

You are configuring a release pipeline in Azure DevOps as shown in the exhibit.

CertyIQ



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.

Hot Area:

#### Answer:

#### Answer Area

How many stages have triggers set?

|   |
|---|
| 0 |
| 1 |
| 2 |
| 3 |
| 4 |
| 5 |
| 6 |
| 7 |

Which component should you modify to enable continuous delivery?

|                              |
|------------------------------|
| The Development stage        |
| The Internal Review stage    |
| The Production stage         |
| The Web Application artifact |

#### Explanation:

Box 1: 7

Box 2: The Internal Review stage

#### Question: 477

CertyIQ

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 Triggers tab of the build pipeline, you select Enable continuous integration.

Does this meet the goal?

A.Yes

B.No

### Answer: A

#### Explanation:

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

1. Select the Triggers tab.
2. Enable Continuous integration.

A continuous integration trigger on a build pipeline indicates that the system should automatically queue a new build whenever a code change is committed.

Reference:

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

Testlet 1 -

Case Study -

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

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

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

To start the case study -

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

Application Architecture -

The company's primary application is a single monolithic retirement fund management system based on ASP.NET web forms that use logic written in VB.NET. Some new sections of the application are written in C#. Variations of the application are created for individual customers. Currently, there are more than 80 live code branches in the application's code base.

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

Architectural Issues -

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

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

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

Customers report that bug reporting is overly complex.

Planned changes -

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

The investment planning applications suite will include one multi-tier web application and two iOS mobile appl

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

Litware wants to become proactive in detecting failures, rather than always waiting for customer bug reports. Technical requirements -

The company's investment planning applications suite must meet the following requirements:

- ⇒ New incoming connections through the firewall must be minimized.
- ⇒ Members of a group named Developers must be able to install packages.
- ⇒ The principle of least privilege must be used for all permission assignments.
- ⇒ A branching strategy that supports developing new functionality in isolation must be used.
- ⇒ Members of a group named Team Leaders must be able to create new packages and edit the permissions of package feeds.
- ⇒ Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use.
- ⇒ By default, all releases must remain available for 30 days, except for production releases, which must be kept for 60 days.
- ⇒ Code quality and release quality are critical. During release, deployments must not proceed between stages if any active bugs are logged against the release.
- ⇒ The mobile applications must be able to call the share pricing service of the existing retirement fund management system. Until the system is upgraded, the service will only support basic authentication over HTTPS.
- ⇒ The required operating system configuration for the test servers changes weekly. Azure Automation State Configuration must be used to ensure that the operating system on each test server is configured the same way when the servers are created and checked periodically.

Current Technical Issue -

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

Azure Automation State Configuration fails to correct the configurations.

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

" target="\_blank" style="word-break: break-all;">>

**Register-AzurermAutomationDscNode**

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

QUESTION 1 -

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

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

Section: [none]

Explanation -

When a release is created from a release pipeline that defines approvals, the deployment stops at each point where approval is required until the specified approver grants approval or rejects the release (or re-assigns the approval to another user).

Scenario: Code quality and release quality are critical. During release, deployments must not proceed between stages if any active bugs are logged against the release.

References:

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

QUESTION 2 -

HOTSPOT -

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.

Hot Area:

Section: [none]

Explanation -

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

Box 1: Set the default retention policy to 30 days

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

Box 2: Set the stage retention policy to 60 days

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

References:

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

Question Set 2 -

QUESTION 1 -

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 -

Section: [none]

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>

QUESTION 2 -

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 -

Section: [none]

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>

QUESTION 3 -

HOTSPOT -

You have a project in 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.

Hot Area:

Section: [none]

Explanation -

Box 1: "Microsoft.Resources/deployments"

Reference a secret with dynamic ID. You need to reference a key vault secret that varies based on the current deployment.

Example:

"resources": [

```
"apiVersion": "2018-05-01",
"name": "dynamicSecret",
"type": "Microsoft.Resources/deployments",
"properties":
"mode": "Incremental",
"templateLink":
```

Box 2: "templateLink"

In your parent template, you add the linked template and pass in a parameter that contains the dynamically generated resource ID.

References:

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

QUESTION 4 -

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

The company uses ServiceNow for change management.

You need to ensure that a change request is processed before any components can be deployed to the production environment.

What are two ways to integrate ServiceNow into the Azure DevOps release pipeline? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Define a deployment control that invokes the ServiceNow REST API.

B. Define a pre-deployment gate before the deployment to the Prod stage.

C. Define a deployment control that invokes the ServiceNow SOAP API.

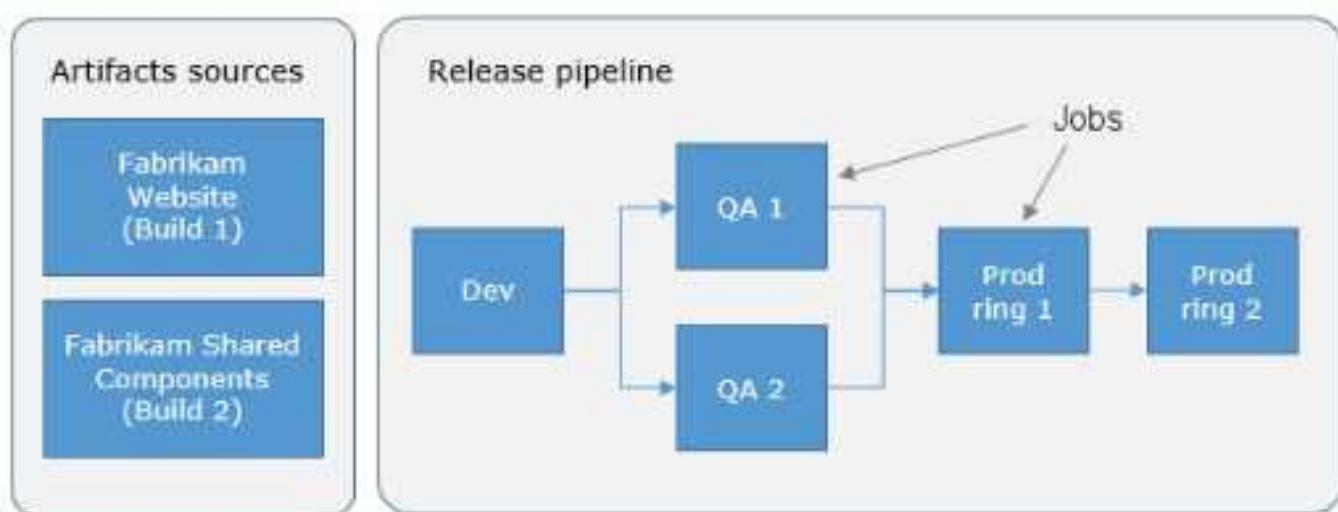
D. Define a post-deployment gate after the deployment to the QA stage.

Section: [none]

Explanation -

An example of a release pipeline that can be modeled through a release pipeline is shown below:

" target="\_blank" style="word-break: break-all;">>



In this example, a release of a website is created by collecting specific versions of two builds (artifacts), each from a different build pipeline. The release is first deployed to a Dev stage and then forked to two QA stages in parallel. If the deployment succeeds in both the QA stages, the release is deployed to Prod ring 1 and then to

Prod ring 2. Each production ring represents multiple instances of the same website deployed at various locations around the globe.

References:

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

QUESTION 5 -

HOTSPOT -

You are configuring a release pipeline in Azure DevOps as shown in the exhibit.

" target="\_blank" style="word-break: break-all;">>



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.

Hot Area:

Section: [none]

Explanation -

Box 1: 5 -

There are five stages: Development, QA, Pre-production, Load Test and Production. They all have triggers.

Box 2: The Internal Review stage

References:

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

QUESTION 6 -

DRAG DROP -

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.

Select and Place:

Section: [none]

Explanation -

Box 1: A deployment group -

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

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

Box 2: A deployment group -

References:

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

QUESTION 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 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 Time between re-evaluation of gates option.

Does this meet the goal?

A. Yes -

B. No -

Section: [none]

Explanation -

Use a gate From Pre-deployment conditions instead.

References:

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

QUESTION 8 -

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.

rect 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 -

Section: [none]

Explanation -

Gates allow automatic collection of health signals from external services, and then promote the release when all the signals are successful at the same time or stop the deployment on timeout. Typically, gates are used in connection with incident management, problem management, change management, monitoring, and external approval systems.

Approvals and gates give you additional control over the start and completion of the deployment pipeline. Each stage in a release pipeline can be configured with pre-deployment and post-deployment conditions that can include waiting for users to manually approve or reject deployments, and checking with other automated systems until specific conditions are verified.

References:

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

QUESTION 9 -

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

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

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

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

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

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

Solution: From Pre-deployment conditions, you modify the Timeout setting for pre-deployment approvals.

Does this meet the goal?

A. Yes -

B. No -

Section: [none]

Explanation -

Use a gate instead of an approval instead.

References:

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

QUESTION 10 -

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 -

Section: [none]

Explanation -

Use a main template and two linked templates.

References:

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

Question Set 1 -

QUESTION 1 -

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

Section: [none]

Explanation -

Upstream sources enable you to manage all of your product's dependencies in a single feed. We recommend publishing all of the packages for a given product to that product's feed, and managing that product's dependencies from remote feeds in the same feed, via upstream sources. This setup has a few benefits:

- ⇒ Simplicity: your NuGet.config, .npmrc, or settings.xml contains exactly one feed (your feed).
- ⇒ Determinism: your feed resolves package requests in order, so rebuilding the same codebase at the same commit or changeset uses the same set of packages
- ⇒ Provenance: your feed knows the provenance of packages it saved via upstream sources, so you can verify that you're using the original package, not a custom or malicious copy published to your feed
- ⇒ Peace of mind: packages used via upstream sources are guaranteed to be saved in the feed on first use; if the upstream source is disabled/removed, or the remote feed goes down or deletes a package you depend on, you can continue to develop and build

References:

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

QUESTION 2 -

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 -

Section: [none]

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 defin

itive database of open source repositories.

Azure DevOps integration with WhiteSource Bolt will enable you to:

1. Detect and remedy vulnerable open source components.
2. Generate comprehensive open source inventory reports per project or build.
3. Enforce open source license compliance, including dependencies licenses.
4. Identify outdated open source libraries with recommendations to update.

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

References:

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

QUESTION 3 -

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

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

What should you use?

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

Section: [none]

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>

Question Set 1 -

QUESTION 1 -

DRAG DROP -

You have an Azure Kubernetes Service (AKS) implementation that is RBAC-enabled.

You plan to use Azure Container Instances as a hosted development environment to run containers in the AKS implementation.

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

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

Select and Place:

Section: [none]

Explanation -

Step 1: Create a YAML file.

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

Step 2: Run kubectl apply.

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

Step 3: Run helm init.

Configure Helm to use the tiller service account:

helm init --service-account tiller

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

References:

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

**Question: 478**

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: Correct C****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>

**Testlet 1 -****Case Study -**

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

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

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

**To start the case study -**

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

**Background -**

Contoso, Ltd. is a manufacturing company that has a main office in Chicago.

Contoso plans to improve its IT development and operations processes by implementing Azure DevOps principles. Contoso has an Azure subscription and creates an Azure DevOps organization.

The Azure DevOps organization includes:

- ⇒ The Docker extension
- ⇒ A deployment pool named Pool7 that contains 10 Azure virtual machines that run Windows Server 2016

The Azure subscription contains an Azure Automation account.

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



Technical requirements -

Contoso identifies the following technical requirements:

- ⇒ Implement build agents for Project1.
- ⇒ Whenever possible, use Azure resources.
- ⇒ Avoid using deprecated technologies.
- ⇒ Implement a code flow strategy for Project2 that will:
  - Enable Team2 to submit pull requests for Project2.
  - Enable Team2 to work independently on changes to a copy of Project2.
  - Ensure that any intermediary changes performed by Team2 on a copy of Project2 will be subject to the same restrictions as the ones defined in the build policy of Project2.
- ⇒ Whenever possible implement automation and minimize administrative effort.
- ⇒ Implement Project3, Project5, Project6, and Project7 based on the planned changes
- ⇒ Implement Project4 and configure the project to push Docker images to Azure Container Registry.

#### QUESTION 1 -

##### HOTSPOT -

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

NOTE: Each correct selection is worth one point.

Hot Area:



" target="\_blank" style="word-break: break-all;">>

```
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"]
```

Section: [none]

Explanation -

Scenario:



References:

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

#### QUESTION 2 -

In Azure DevOps, you create Project3.

You need to meet the requirements of the project.

What should you do first?

- A. From Azure DevOps, modify the build definition.
- B. From SonarQube, obtain an authentication token.
- C. From Azure DevOps, create a service endpoint.
- D. From SonarQube, create a project.

Section: [none]

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>

Question Set 2 -

#### QUESTION 1 -

DRAG DROP -

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

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

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

Select and Place:

Section: [none]

Explanation -

Step 1: Assign the node configuration.

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

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

You import the configuration into the Automation account.

Step 3: Compiling a configuration into a node configuration

Compiling a configuration in Azure Automation

Before you can apply a desired state to a node, a DSC configuration defining that state must be compiled into one or more node configurations (MOF document), and placed on the Automation DSC Pull Server.

Step 4: Onboard the virtual machines to Azure State Configuration

Onboarding an Azure VM for management with Azure Automation State Configuration

Step 5: Check the compliance status of the node.

Viewing reports for managed nodes. Each time Azure Automation State Configuration performs a consistency check on a managed node, the node sends a status report back to the pull server. You can view these reports on the page for that node.

On the blade for an individual report, you can see the following status information for the corresponding consistency check:

The report status whether the node is "Compliant", the configuration "Failed", or the node is "Not Compliant" (when the node is in ApplyandMonitor mode and the machine is not in the desired state).

References:

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

QUESTION 2 -

You have 50 Node.js-based projects that you scan by using WhiteSource. Each project includes Package.json, Package-lock.json, and Npm-shrinkwrap.json files.

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

What should you do?

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

Section: [none]

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-security-as-reported-by-your-cicd-pipeline/>

QUESTION 3 -

Your company deploys applications in Docker containers.

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

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

What should you configure?

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

Section: [none]

Explanation -

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

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

Incorrect Answers:

C: We should not wait until deployment. We want to detect the exploits as early as possible.

D: We should wait until the image is in the product container. We want to detect the exploits as early as possible.

References:

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

QUESTION 4 -

Your company uses Azure DevOps for the build pipelines and deployment pipelines of Java-based projects.

You need to recommend a strategy for managing technical debt.

Which two actions should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Section: [none]

Explanation -

QUESTION 5 -

Your company has a hybrid cloud between Azure and Azure Stack.

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

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

The solution must minimize management overhead.

What should you use to execute the build pipeline?

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

Section: [none]

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>

QUESTION 6 -

You need to recommend a Docker container build strategy that meets the following requirements:

- ⇒ Minimizes image sizes
- ⇒ Minimizes the security surface area of the final image

What should you include in the recommendation?

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

Section: [none]

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.

Incorrect Answers:

C: A swarm consists of multiple Docker hosts which run in swarm mode and act as managers (to manage membership and delegation) and workers (which run swarm services).

References:

<https://docs.docker.com/develop/develop-images/multistage-build/>

QUESTION 7 -

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. NUnit -
- C. Coverage.py -
- D. Coverlet -

Section: [none]

Explanation -

Use Publish Code Coverage Results task in a build pipeline to publish code coverage results to Azure Pipelines or TFS, which were produced by a build in Cobertura or JaCoCo format.

References:

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

QUESTION 8 -

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.)

" target="\_blank" style="word-break: break-all;">>

```
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 -

Section: [none]

Explanation -

Multi-stage builds (in Docker 17.05 or higher) allow you to drastically reduce the size of your final image, without struggling to reduce the number of intermediate layers and files.

With multi-stage builds, you use multiple FROM statements in your Dockerfile. Each FROM instruction can use a different base, and each of them begins a new stage of the build. You can selectively copy artifacts from one stage to another, leaving behind everything you don't want in the final image.

References:

<https://docs.docker.com/develop/develop-images/multistage-build/#use-multi-stage-builds>

QUESTION 9 -

You are developing an open source solution that uses a GitHub repository.

You create a new public project in Azure DevOps.

You plan to use Azure Pipelines for continuous build. The solution will use the GitHub Checks API.

Which authentication type should you use?

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

Section: [none]

Explanation -

You can authenticate as a GitHub App.

References:

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

QUESTION 10 -

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 -

Section: [none]

Explanation -

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

1. Select the Triggers tab.
2. Enable Continuous integration.

References:

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

QUESTION 11 -

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 -

Section: [none]

Explanation -

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

1. Select the Triggers tab.
2. Enable Continuous integration.

References:

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

QUESTION 12 -

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 -

Section: [none]

Explanation -

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

1. Select the Triggers tab.
2. Enable Continuous integration.

References:

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

QUESTION 13 -

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 Triggers tab of the build pipeline, you select Enable continuous integration.

Does this meet the goal?

A. Yes -

B. No -

Section: [none]

Explanation -

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

1. Select the Triggers tab.
2. Enable Continuous integration.

A continuous integration trigger on a build pipeline indicates that the system should automatically queue a new build whenever a code change is committed.

References:

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

Testlet 1 -

Case Study -

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

d.

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

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

To start the case study -

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

Application Architecture -

The company's primary application is a single monolithic retirement fund management system based on ASP.NET web forms that use logic written in VB.NET. Some new sections of the application are written in C#. Variations of the application are created for individual customers. Currently, there are more than 80 live code branches in the application's code base.

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

Architectural Issues -

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

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

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

Customers report that bug reporting is overly complex.

Planned changes -

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

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

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

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

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

Technical requirements -

The company's investment planning applications suite must meet the following requirements:

- ⇒ New incoming connections through the firewall must be minimized.
- ⇒ Members of a group named Developers must be able to install packages.
- ⇒ The principle of least privilege must be used for all permission assignments.
- ⇒ A branching strategy that supports developing new functionality in isolation must be used.
- ⇒ Members of a group named Team Leaders must be able to create new packages and edit the permissions of package feeds.
- ⇒ Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use.
- ⇒ By default, all releases must remain available for 30 days, except for production releases, which must be kept for 60 days.
- ⇒ Code quality and release quality are critical. During release, deployments must not proceed between stages if any active bugs are logged against the release.

- ⇒ The mobile applications must be able to call the share pricing service of the existing retirement fund management system. Until the system is upgraded, the service will only support basic authentication over HTTPS.
- ⇒ The required operating system configuration for the test servers changes weekly. Azure Automation State Configuration must be used to ensure that the operating system on each test server is configured the same way when the servers are created and checked periodically.

Current Technical Issue -

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

Azure Automation State Configuration fails to correct the configurations.

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



QUESTION 1 -

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

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

Section: [none]

Explanation -

When a release is created from a release pipeline that defines approvals, the deployment stops at each point where approval is required until the specified approver grants approval or rejects the release (or re-assigns the approval to another user).

Scenario: Code quality and release quality are critical. During release, deployments must not proceed between stages if any active bugs are logged against the release.

References:

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

QUESTION 2 -

HOTSPOT -

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.

Hot Area:

Section: [none]

Explanation -

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

Box 1: Set the default retention policy to 30 days

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

Box 2: Set the stage retention policy to 60 days

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

References:

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

Question Set 2 -

QUESTION 1 -

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 temp

lates. 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 -

Section: [none]

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>

QUESTION 2 -

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 -

Section: [none]

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>

QUESTION 3 -

HOTSPOT -

You have a project in 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.

Hot Area:

Section: [none]

Explanation -

Box 1: "Microsoft.Resources/deployments"

Reference a secret with dynamic ID. You need to reference a key vault secret that varies based on the current

deployment.

Example:

"resources": [

```
"apiVersion": "2018-05-01",
"name": "dynamicSecret",
"type": "Microsoft.Resources/deployments",
"properties":
"mode": "Incremental",
"templateLink":
```

Box 2: "templateLink"

In your parent template, you add the linked template and pass in a parameter that contains the dynamically generated resource ID.

References:

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

QUESTION 4 -

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

The company uses ServiceNow for change management.

You need to ensure that a change request is processed before any components can be deployed to the production environment.

What are two ways to integrate ServiceNow into the Azure DevOps release pipeline? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Define a deployment control that invokes the ServiceNow REST API.
- B. Define a pre-deployment gate before the deployment to the Prod stage.
- C. Define a deployment control that invokes the ServiceNow SOAP API.
- D. Define a post-deployment gate after the deployment to the QA stage.

Section: [none]

Explanation -

An example of a release pipeline that can be modeled through a release pipeline is shown below:



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

References:

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

QUESTION 5 -

HOTSPOT -

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.

Hot Area:

Section: [none]

Explanation -

Box 1: 5 -

There are five stages: Development, QA, Pre-production, Load Test and Production. They all have triggers.

Box 2: The Internal Review stage

References:

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

QUESTION 6 -

DRAG DROP -

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.

Select and Place:

Section: [none]

Explanation -

Box 1: A deployment group -

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

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

Box 2: A deployment group -

References:

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

QUESTION 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 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 Time between re-evaluation of gates option.

Does this meet the goal?

A. Yes -

B. No -

Section: [none]

Explanation -

Use a gate From Pre-deployment conditions instead.

References:

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

QUESTION 8 -

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 -

Section: [none]

Explanation -

Gates allow automatic collection of health signals from external services, and then promote the release when all the signals are successful at the same time or stop the deployment on timeout. Typically, gates are used in connection with incident management, problem management, change management, monitoring, and external approval systems.

Approvals and gates give you additional control over the start and completion of the deployment pipeline. Each stage in a release pipeline can be configured with pre-deployment and post-deployment conditions that can include waiting for users to manually approve or reject deployments, and checking with other automated systems until specific conditions are verified.

References:

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

QUESTION 9 -

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

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

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

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

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

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

Solution: From Pre-deployment conditions, you modify the Timeout setting for pre-deployment approvals.

Does this meet the goal?

A. Yes -

B. No -

Section: [none]

Explanation -

Use a gate instead of an approval instead.

References:

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

QUESTION 10 -

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 -

Section: [none]

Explanation -

Use a main template and two linked templates.

References:

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

Question Set 1 -

QUESTION 1 -

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. local symbols -

B. views -

C. global symbols -

D. upstream sources -

Section: [none]

Explanation -

Upstream sources enable you to manage all of your product's dependencies in a single feed. We recommend publishing all of the packages for a given product to that product's feed, and managing that product's dependencies from remote feeds in the same feed, via upstream sources. This setup has a few benefits:

- ⇒ Simplicity: your NuGet.config, .npmrc, or settings.xml contains exactly one feed (your feed).
- ⇒ Determinism: your feed resolves package requests in order, so rebuilding the same codebase at the same commit or changeset uses the same set of packages
- ⇒ Provenance: your feed knows the provenance of packages it saved via upstream sources, so you can verify that you're using the original package, not a custom or malicious copy published to your feed
- ⇒ Peace of mind: packages used via upstream sources are guaranteed to be saved in the feed on first use; if the upstream source is disabled/removed, or the remote feed goes down or deletes a package you depend on, you can continue to develop and build

References:

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

QUESTION 2 -

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 -

Section: [none]

Explanation -

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

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

Azure DevOps integration with WhiteSource Bolt will enable you to:

1. Detect and remedy vulnerable open source components.
2. Generate comprehensive open source inventory reports per project or build.
3. Enforce open source license compliance, including dependencies licenses.

4. Identify outdated open source libraries with recommendations to update.

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

References:

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

### QUESTION 3 -

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

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

What should you use?

A. Microsoft Visual SourceSafe -

B. Code Style -

C. Black Duck -

D. Jenkins -

Section: [none]

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>

Question Set 1 -

### QUESTION 1 -

DRAG DROP -

You have an Azure Kubernetes Service (AKS) implementation that is RBAC-enabled.

You plan to use Azure Container Instances as a hosted development environment to run containers in the AKS implementation.

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

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

Select and Place:

Section: [none]

Explanation -

Step 1: Create a YAML file.

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

Step 2: Run kubectl apply.

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

Step 3: Run helm init.

Configure Helm to use the tiller service account:

helm init --service-account tiller

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

References:

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

Question Set 1

Your company creates a web application.

You need to recommend a solution that automatically sends to Microsoft Teams a daily summary of the exceptions that occur in the application.

Which two Azure services should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A.Azure Logic Apps

B.Azure Pipelines

C.Microsoft Visual Studio App Center

D.Azure DevOps Project

E.Azure Application Insights

#### Answer: AE

#### Explanation:

E: Exceptions in your live web app are reported by Application Insights.

Note: Periodical reports help keep a team informed on how their business critical services are doing.

Developers, DevOps/SRE teams, and their managers can be productive with automated reports reliably delivering insights without requiring everyone to sign in the portal. Such reports can also help identify gradual increases in latencies, load or failure rates that may not trigger any alert rules.

A: You can programmatically query Application Insights data to generate custom reports on a schedule. The following options can help you get started quickly:

Automate reports with Microsoft Flow

- 
- ⇒ Automate reports with Logic Apps

Reference:

<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>

CertyIQ

#### Question: 480

To resolve the current technical issue, what should you do to the Register-AzureRmAutomationDscNode command?

A.Change the value of the ConfigurationMode parameter.

B.Replace the Register-AzureRmAutomationDscNode cmdlet with Register-AzureRmAutomationScheduledRunbook

C.Add the AllowModuleOverwrite parameter.

D.Add the DefaultProfile parameter.

#### Answer: A

#### Explanation:

Change the ConfigurationMode parameter from ApplyOnly to ApplyAndAutocorrect.

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

Scenario: Current Technical Issue

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

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

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

Reference:

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

### Question: 481

CertyIQ

HOTSPOT -

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 is worth one point.

Hot Area:

## Answer Area

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

|                     |
|---------------------|
| [MSAnalytics.self,  |
| [MSDistribute.self, |
| [MSPush.self,       |

|                    |
|--------------------|
| MSAnalytics.self]  |
| MSCrashes.self]    |
| MSDistribute.self] |

Answer:

## Answer Area

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

|                     |
|---------------------|
| [MSAnalytics.self,  |
| [MSDistribute.self, |
| [MSPush.self,       |

|                    |
|--------------------|
| MSAnalytics.self]  |
| MSCrashes.self]    |
| MSDistribute.self] |

### Explanation:

Scenario: Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use.

In order to use App Center, you need to opt in to the service(s) that you want to use, meaning by default no services are started and you will have to explicitly call each of them when starting the SDK.

Insert the following line to start the SDK in your app's AppDelegate class in the didFinishLaunchingWithOptions method.

```
MSAppCenter.start(" Your App Secret ", withServices: [MSAnalytics.self, MSCrashes.self])
```

Reference:

<https://docs.microsoft.com/en-us/appcenter/sdk/getting-started/ios>

CertyIQ

### Question: 482

You add the virtual machines as managed nodes in Azure Automation State Configuration.

You need to configure the computers in Group7.

What should you do?

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

**Answer: B**

**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. |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode>

CertyIQ

### Question: 483

DRAG DROP -

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

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

Select and Place:

**Answer:**

## Actions

Create a fork

Add a build policy

## Answer Area

Create a fork

Create a branch

Add a build policy



Add an application access policy.

### Explanation:

Step 1: Create a fork

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 policy

## Question: 484

CertyIQ

DRAG DROP -

You need to configure Azure Automation for the computers 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.

Select and Place:

### Actions

### Answer Area

Run the Import-AzureRmAutomationDscConfiguration Azure PowerShell cmdlet.

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

Run the New-AzureRmResourceGroupDeployment Azure PowerShell cmdlet.

Run the Start-AzureRmAutomationDscCompilationJob Azure PowerShell cmdlet.

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



### Answer:

**Actions****Answer Area**

Run the New-AzureRmResourceGroupDeployment Azure PowerShell cmdlet.

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

Run the Import-AzureRmAutomationDscConfiguration Azure PowerShell cmdlet.

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

Run the Start-AzureRmAutomationDscCompilationJob Azure PowerShell cmdlet.

**Explanation:**

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

Step 2: Run the Import-AzureRmAutomationDscConfiguration Azure Powershell cmdlet

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

Example:

```
PS C:\>Import-AzureRmAutomationDscConfiguration -AutomationAccountName "Contoso17" -
ResourceGroupName "ResourceGroup01" -SourcePath "C:\DSC
\client.ps1" -Force
```

This command imports the DSC configuration in the file named client.ps1 into the Automation account named Contoso17. The command specifies the Force parameter. If there is an existing DSC configuration, this command replaces it.

Step 3: Run the Start-AzureRmAutomationDscCompilationJob Azure Powershell cmdlet

The Start-AzureRmAutomationDscCompilationJob cmdlet compiles an APS Desired State Configuration (DSC) configuration in Azure Automation.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/import-azurermautomationdscconfiguration> <https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/start-azurermautomationdsccompilationjob>

**Question: 485****CertyIQ**

HOTSPOT -

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

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:

## Answer Area

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   |

@

Explanation:

In the branch filter I cannot see \, only the branch names like master or branch1. I guess if you want to add

path (like \) you need to use path filters. So 1. Path filter to exclude 2. Path filter to include

References:

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

CertyIQ

### Question: 486

You use a Git repository in Azure Repos to manage the source code of a web application. Developers commit changes directly to the master branch.

You need to implement a change management procedure that meets the following requirements:

- ⇒ The master branch must be protected, and new changes must be built in the feature branches first.
- ⇒ Changes must be reviewed and approved by at least one release manager before each merge.
- ⇒ Changes must be brought into the master branch by using pull requests.

What should you configure in Azure Repos?

A. branch policies of the master branch

B. Services in Project Settings

C. Deployment pools in Project Settings

D. branch security of the master branch

### Answer: A

#### Explanation:

Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.

Reference:

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

CertyIQ

### Question: 487

You have a free tier of an Azure DevOps organization named Contoso. Contoso contains 10 private projects. Each project has multiple jobs with no dependencies.

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

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

What should you do?

A. Configure the pipelines to use the Microsoft-hosted agents.

B. Register additional self-hosted agents.

C. Purchase self-hosted parallel jobs.

D. Purchase Microsoft-hosted parallel jobs.

### Answer: C

#### Explanation:

C. Purchase self-hosted parallel jobs

It should be C- as the it talks about jobs running on a self-hosted pool in question.

## Question: 488

CertyIQ

You have a private distribution group that contains provisioned and unprovisioned devices.

You need to distribute a new iOS application to the distribution group by using Microsoft Visual Studio App Center. What should you do?

- A.Generate a new .p12 file for each device.
- B.Create an unsigned build.
- C.Register the devices on the Apple Developer portal.**
- D.Create an active subscription in App Center Test.

### Answer: C

#### Explanation:

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

Reference:

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

## Question: 489

CertyIQ

You have a Microsoft ASP.NET Core web app in Azure that is accessed worldwide.

You need to run a URL ping test once every five minutes and create an alert when the web app is unavailable from specific Azure regions. The solution must minimize development time.

What should you do?

- A.Create an Azure Monitor Availability metric and alert.
- B.Create an Azure Application Insights availability test and alert.**
- C.Write an Azure function and deploy the function to the specific regions.
- D.Create an Azure Service Health alert for the specific regions.

### Answer: B

#### Explanation:

There are three types of Application Insights availability tests:

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

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

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

You don't have to make any changes to the website you're testing. In fact, it doesn't even have to be a site you own. You can test the availability of a REST API that your service depends on.

Reference:

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

### Question: 490

CertyIQ

DRAG DROP -

You need to replace the existing DevOps tools to support the planned changes.

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

NOTE: Each correct selection is worth one point.

Select and Place:

#### Tools

Azure Boards

Azure Artifacts

GitHub Actions

Azure Pipelines

Azure Test Plans

GitHub repositories

#### Answer Area

Trello:

Tool

Bamboo:

Tool

BitBucket:

Tool

Answer:

#### Tools

Azure Artifacts

GitHub Actions

Azure Test Plans

#### Answer Area

Trello:

Azure Boards

Bamboo:

Azure Pipelines

BitBucket:

GitHub repositories

Explanation:

#### Box 1: Azure Boards -

Azure Boards can be used to track work with Kanban boards, backlogs, team dashboards, and custom reporting

You can create multiple Trello boards, which are spaces to store tasks (for different work contexts, or even private boards)

You can easily share Trello boards with another person.

#### Box 2: Azure Pipelines -

You can use Bamboo to implement CI/CD (Continuous Integration and Continuous Delivery) for a simple Azure function app using Atlassian Bamboo. Bamboo does continuous delivery of the project from source code to deployment. It has stages including Build, Test and Deploy.

Software teams in every industry are upgrading their continuous delivery pipeline with Bamboo. Easy build import from popular open source tools, user and group import from JIRA, seamless integration with Bitbucket, and native support for Git, Hg, and SVN means you'll be building and deploying like a champ.

#### Box 3: GitHub repositories -

Bitbucket can be used as the Git repository, but you can use any other Git repository (Like TFS Git) for source control of the code.

#### Reference:

<https://www.trustradius.com/compare-products/azure-devops-services-vs-trello> <https://marketplace.visualstudio.com/items?itemName=ms-vsts.vss-services-bamboo> <https://www.c-sharpcorner.com/article/cicd-implementation-for-an-azure-function-app-using-atlassian-bamboo-server/>

### Question: 491

CertyIQ

You need to merge the POC branch into the default branch. The solution must meet the technical requirements.

Which command should you run?

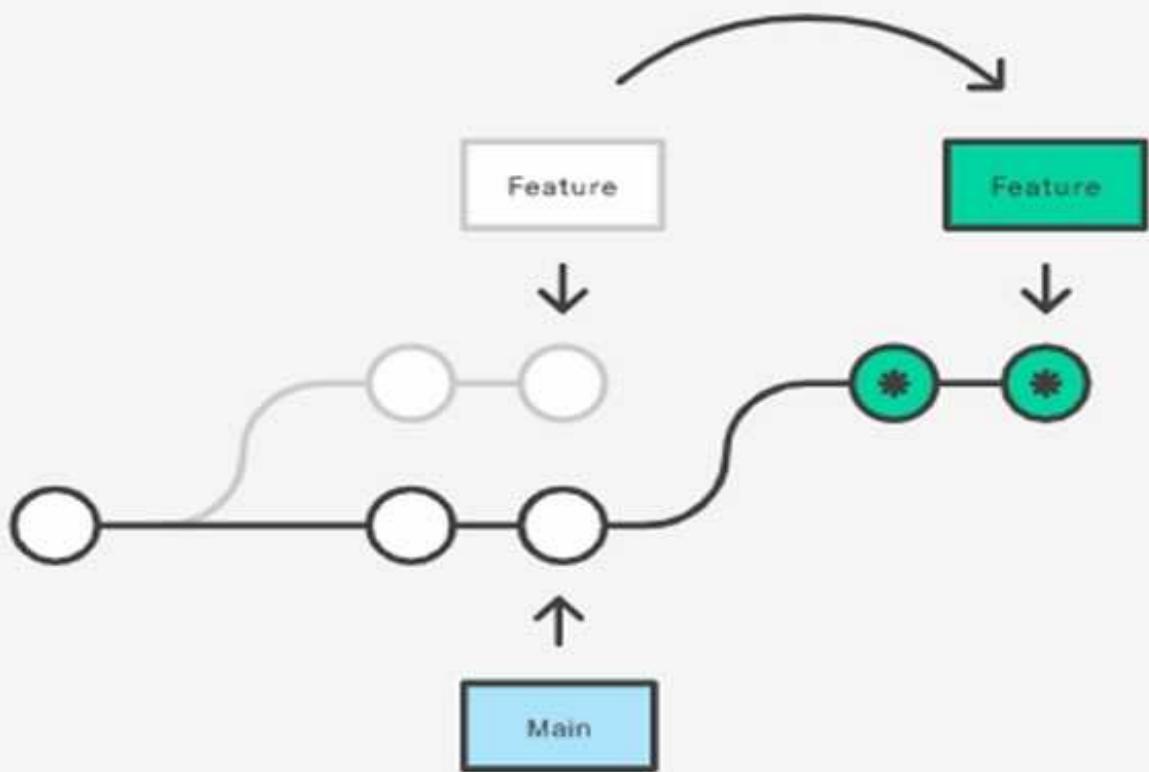
- A.git rebase
- B.git merge --squash
- C.git push
- D.git merge --allow-unrelated-histories

#### Answer: A

#### Explanation:

The commit history of the POC branch must replace the history of the default branch.

Rebasing is the process of moving or combining a sequence of commits to a new base commit. Rebasing is most useful and easily visualized in the context of a feature branching workflow. The general process can be visualized as the following:



Note: The primary reason for rebasing is to maintain a linear project history. For example, consider a situation where the main branch has progressed since you started working on a feature branch. You want to get the latest updates to the main branch in your feature branch, but you want to keep your branch's history clean so it appears as if you've been working off the latest main branch. This gives the later benefit of a clean merge of your feature branch back into the main branch. Why do we want to maintain a "clean history"? The benefits of having a clean history become tangible when performing Git operations to investigate the introduction of a regression.

Incorrect:

Not B: git-merge - Join two or more development histories together.

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 adds all the file changes to a single new commit on the default branch.

Not D: git merge --allow-unrelated-histories

By default, git merge command refuses to merge histories that do not share a common ancestor. This option can be used to override this safety when merging histories of two projects that started their lives independently. As that is a very rare occasion, no configuration variable to enable this by default exists and will not be added.

Reference:

<https://www.atlassian.com/git/tutorials/rewriting-history/git-rebase>

## Question: 492

CertyIQ

You need to perform the GitHub code migration. The solution must support the planned changes for the DevOps environment.

What should you use?

- A.git clone
- B.GitHub Importer
- C.Import repository in Azure Repos
- D.git-tfs

**Answer: B**

**Explanation:**

The git-tfs tool is used for migrating TFSC to Git (within Azure Devops). But in this case we need to "Migrate all the source code from TFS1 to GitHub." And GitHub is another product (using git as version control system). To migrate tfsc to GitHub, your best option would be the GitHub Importer."About GitHub Importer - If you have source code in Subversion, Mercurial, Team Foundation Version Control (TFVC), or another Git repository, you can move it to GitHub using GitHub Importer."<https://docs.microsoft.com/en-us/devops/develop/git/migrate-from-tfvc-to-git><https://docs.github.com/en/get-started/importing-your-projects-to-github/importing-source-code-to-github/about-github-importer>

<https://docs.github.com/en/get-started/importing-your-projects-to-github/importing-source-code-to-github/about-github-importer>

**Question: 493**

CertyIQ

HOTSPOT -

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Set a

|                          |
|--------------------------|
| branch filter to exclude |
| branch filter to include |
| path filter to exclude   |
| path filter to include   |

/folder1.

Set a

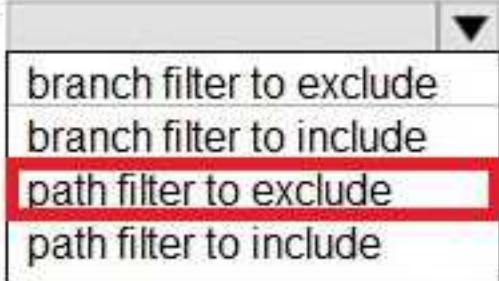
|                          |
|--------------------------|
| branch filter to exclude |
| branch filter to include |
| path filter to exclude   |
| path filter to include   |

/

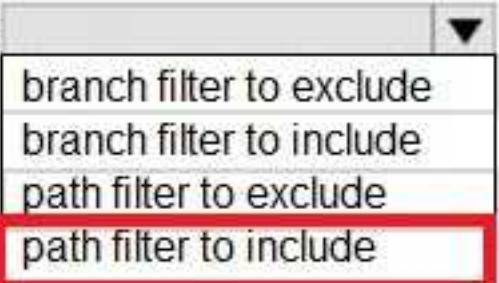
@

**Answer:**

## Answer Area

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**

@

### Explanation:

Path filter to exclude

path filter to include

## Question: 494

CertyIQ

In Azure DevOps, you create Project3.

You need to meet the requirements of the project.

What should you do first?

- A.From Azure DevOps, modify the build definition.
- B.From SonarQube, obtain an authentication token.**
- C.From Azure DevOps, create a service endpoint.
- D.From SonarQube, create a project.

### Answer: B

### Explanation:

B is the answer

<https://learn.microsoft.com/en-us/azure/devops/pipelines/tasks/reference/sonar-qube-prepare-v5?view=azure-pipelines> Specifies the SonarQube server endpoint for your project. To create one, click the Manage link, create a new SonarQube Server Endpoint, and enter your server url and token.

When you create the service endpoint you'll be asked the AuthenticationToken read from <https://docs.sonarqube.org/latest/analysis/azuredevops-integration/#header-3> "Adding a new SonarQube Service Endpoint After installing your extension, you need to declare your SonarQube server as a service

endpoint in your Azure DevOps project settings:"In Azure DevOps, go to Project Settings > Service connections.Click New service connection and select SonarQube from the service connection list.Enter your SonarQube Server URL, an Authentication Token, and a memorable Service connection name. Then, click Save."the link of "Authentication Token" points indeed to SonarQube url <https://docs.sonarqube.org/latest/user-guide/user-token/> where it is documented how to obtain the token from them.hence the answer is clearly B: From SonarQube, obtain an authentication token.

### Question: 495

CertyIQ

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.

Reference:

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

### Question: 496

CertyIQ

DRAG DROP -

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.

Select and Place:

## Actions

Sign in to Azure DevOps by using an account that is assigned the Administrator service connection security role.

Install the Azure Pipelines agent on on-premises virtual machine.

Create a personal access token in the Azure DevOps organization of Contoso.

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

Sign in to Azure DevOps by using an account that is assigned the agent pool administrator role.

## Answer Area

### Answer:

#### Actions

Sign in to Azure DevOps by using an account that is assigned the Administrator service connection security role.

Install the Azure Pipelines agent on on-premises virtual machine.

Create a personal access token in the Azure DevOps organization of Contoso.

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

Sign in to Azure DevOps by using an account that is assigned the agent pool administrator role.

#### Answer Area

Sign in to Azure DevOps by using an account that is assigned the Administrator service connection security role.

Create a personal access token in the Azure DevOps organization of Contoso.

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

### Explanation:

#### Scenario:

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

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

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

Step 2: Create a personal access token..

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

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

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

Reference:

<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/>

CertyIQ

### Question: 497

DRAG DROP -

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.

Select and Place:

#### Actions

#### Answer Area

Open the release pipeline editor.

Disable the continuous integration trigger.

Enable Gates.

Add a manual intervention task.

Open the **Triggers** tab.

Add Query Work Items.



Answer:

#### Actions

#### Answer Area

Open the release pipeline editor.

Open the release pipeline editor.

Disable the continuous integration trigger.

Enable Gates.

Enable Gates.

Add Query Work Items.



Add a manual intervention task.

Open the **Triggers** tab.

Add Query Work Items.

#### Explanation:

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

**Project 6**

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

Step 1: Open the release pipeline editor.

In the Releases tab of Azure Pipelines, select your release pipeline and choose Edit to open the pipeline editor.

Step 2: Enable Gates.

Choose the pre-deployment conditions icon for the Production stage to open the conditions panel. Enable gates by using the switch control in the Gates section.

Step 3: Add Query Work items.

Choose + Add and select the Query Work Items gate.

Configure the gate by selecting an existing work item query.

## Deployment gates ⓘ

+ Add ▾

### Query Work Items

Enabled



Query Work Items ⓘ

Task version  ▾

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.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deploy-using-approvals?view=azure-devops#configure-gate>

To resolve the current technical issue, what should you do to the Register-AzureRmAutomationDscNode command?

- A.Change the value of the ConfigurationMode parameter.
- B.Replace the Register-AzureRmAutomationDscNode cmdlet with Register-AzureRmAutomationScheduledRunbook
- C.Add the AllowModuleOverwrite parameter.
- D.Add the DefaultProfile parameter.

**Answer: A****Explanation:**

Change the ConfigurationMode parameter from ApplyOnly to ApplyAndAutocorrect.

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

Scenario: Current Technical Issue

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

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

**Register-AzureRmAutomationDscNode**

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

Reference:

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

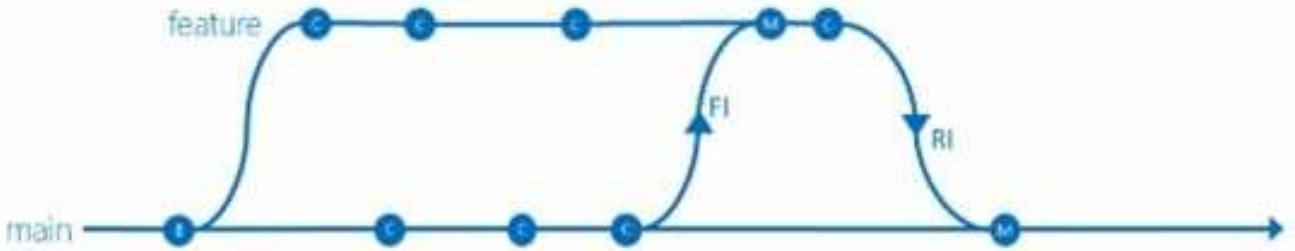
Which branching strategy should you recommend for the investment planning applications suite?

- A.release isolation
- B.main only
- C.development isolation
- D.feature isolation

**Answer: D****Explanation:**

Scenario: A branching strategy that supports developing new functionality in isolation must be used.

Feature isolation is a special derivation of the development isolation, allowing you to branch one or more feature branches from main, as shown, or from your dev branches.



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

Incorrect Answers:

- A: Release isolation introduces one or more release branches from main. The strategy allows concurrent release management, multiple and parallel releases, and codebase snapshots at release time.
- B: The Main Only strategy can be folder-based or with the main folder converted to a Branch, to enable additional visibility features. You commit your changes to the main branch and optionally indicate development and release milestones with labels.
- C: Development isolation: When you need to maintain and protect a stable main branch, you can branch one or more dev branches from main. It enables isolation and concurrent development. Work can be isolated in development branches by feature, organization, or temporary collaboration.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/branching-strategies-with-tfvc?view=azure-devops>

## Question: 500

CertyIQ

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

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

**Answer: B**

**Explanation:**

"Code quality and release quality are critical. During release, deployments must not proceed between stages if any active bugs are logged against the release."

"<https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/?view=azure-devops>" A team wants to ensure there are no active issues in the work item or problem management system before deploying a build to a stage.Pre-deployment gates" Answer is B

Correct answer should be B. Use quality gates

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

## Question: 501

CertyIQ

HOTSPOT -

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.

Hot Area:

## Answer Area

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:

## Answer Area

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.

Explanation:

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

Box 1: Set the default retention policy to 30 days

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

Box 2: Set the stage retention policy to 60 days

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

Reference:

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

### Question: 502

CertyIQ

HOTSPOT -

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

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:

## Answer Area

Build agent:

- A hosted service
- A source control system
- The developers' computers

Release agent:

- A hosted service
- A source control system
- The developers' computers

### Explanation:

Box 1: A source control system -

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

Box 2: A hosted service -

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

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

Reference:

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

# Thank you

Thank you for being so interested in the premium exam material.

I'm glad to hear that you found it informative and helpful.

If you have any feedback or thoughts on the bumps, I would love to hear them.  
Your insights can help me improve our writing and better understand our readers.

## Best of Luck

You have worked hard to get to this point, and you are well-prepared for the exam  
Keep your head up, stay positive, and go show that exam what you're made of!

[Feedback](#)

[More Papers](#)



Future is Secured

100% Pass Guarantee



24/7 Customer Support

Mail us - [certyiqofficial@gmail.com](mailto:certyiqofficial@gmail.com)



Free Updates

Lifetime Free Updates!

Total: **502 Questions**

Link: <https://certyiq.com/papers?provider=microsoft&exam=az-400>