1 Topic 1 - Question Set 1

Question #1*Topic 1*

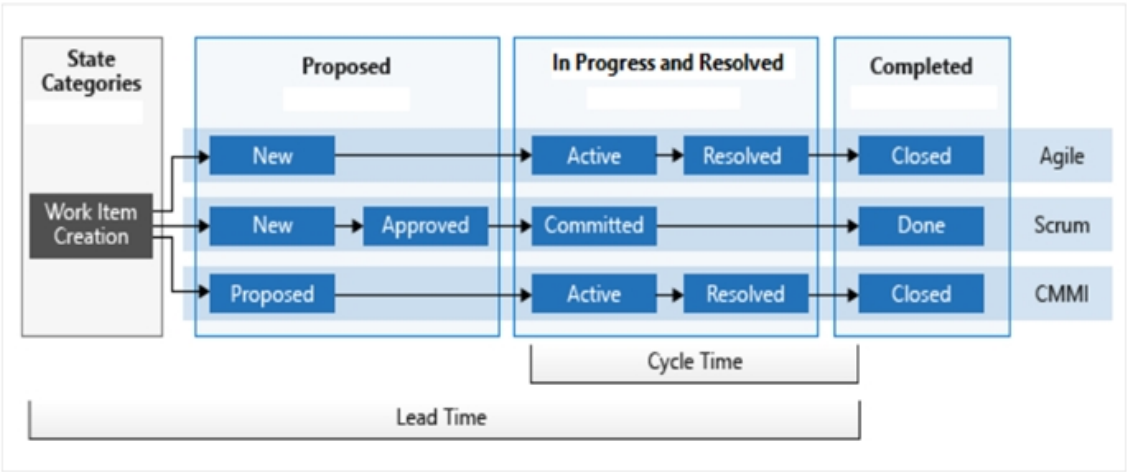
You are configuring project metrics for dashboards in Azure DevOps.
You need to configure a chart widget that measures the elapsed time to complete work items once they become active.
Which of the following is the widget you should use?

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

Hide Solution | Discussion 11

Correct Answer: *C*
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.



Community vote distribution
C (100%)

Question #2*Topic 1*

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 **Most Voted**
- C. Test results trend
- D. Burndown

Hide Solution Discussion 10

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

Community vote distribution

B (100%)

Question #3*Topic 1*

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 **Most Voted**

Hide Solution Discussion 16

Correct Answer: *D*

Community vote distribution

D (69%)
A (31%)

Question #4*Topic 1*

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

Hide Solution Discussion 6

Correct Answer: *B*
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

> **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.

Community vote distribution

B (100%)

Question #5*Topic 1*

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. **Most Voted**
- C. Upgrading PowerShell Core to the latest version.
- D. Using the TFS Integration Platform to perform the upgrade.

Hide Solution | Discussion 7

Correct Answer: *B*
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.

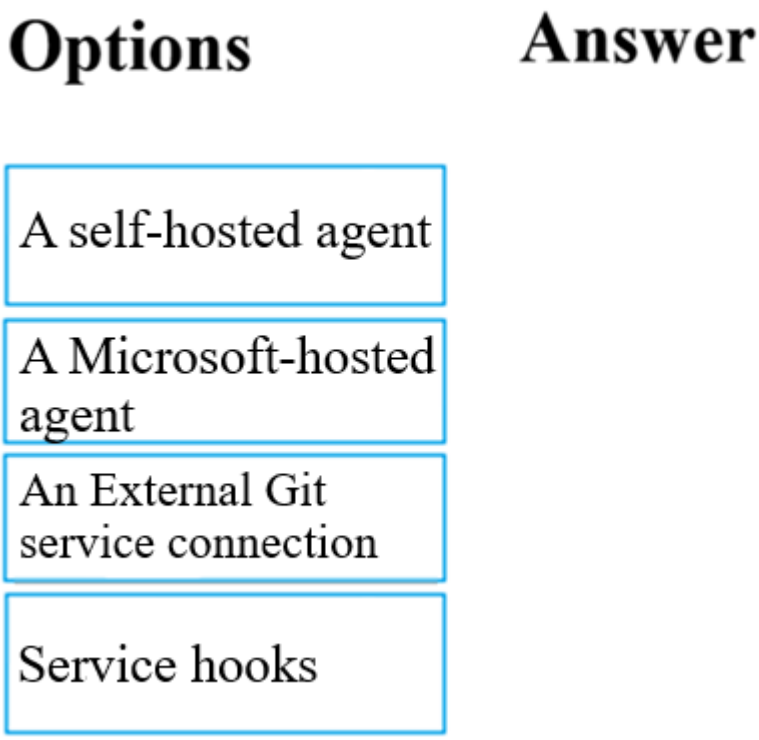
Community vote distribution

B (100%)

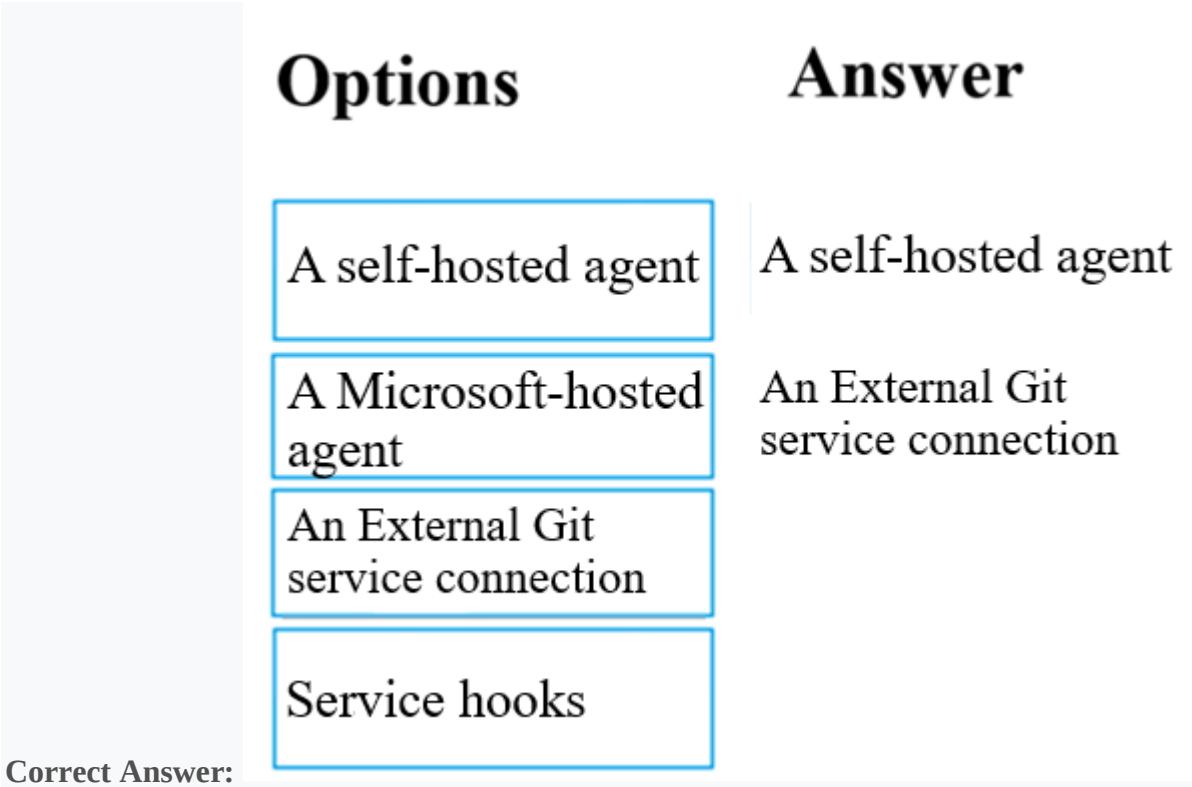
Question #6*Topic 1*

DRAG DROP -
You have an on-premises Bitbucket Server with a firewall configured to block inbound

Internet traffic. The server is used for Git-based source control.
You intend to manage the build and release processes using Azure DevOps. This plan requires you to integrate Azure DevOps and Bitbucket.
Which of the following will allow for this integration? Answer by dragging the correct options from the list to the answer area.
Select and Place:



Hide Solution Discussion 11



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

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

Question #7*Topic 1*

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

Reveal Solution Discussion 9

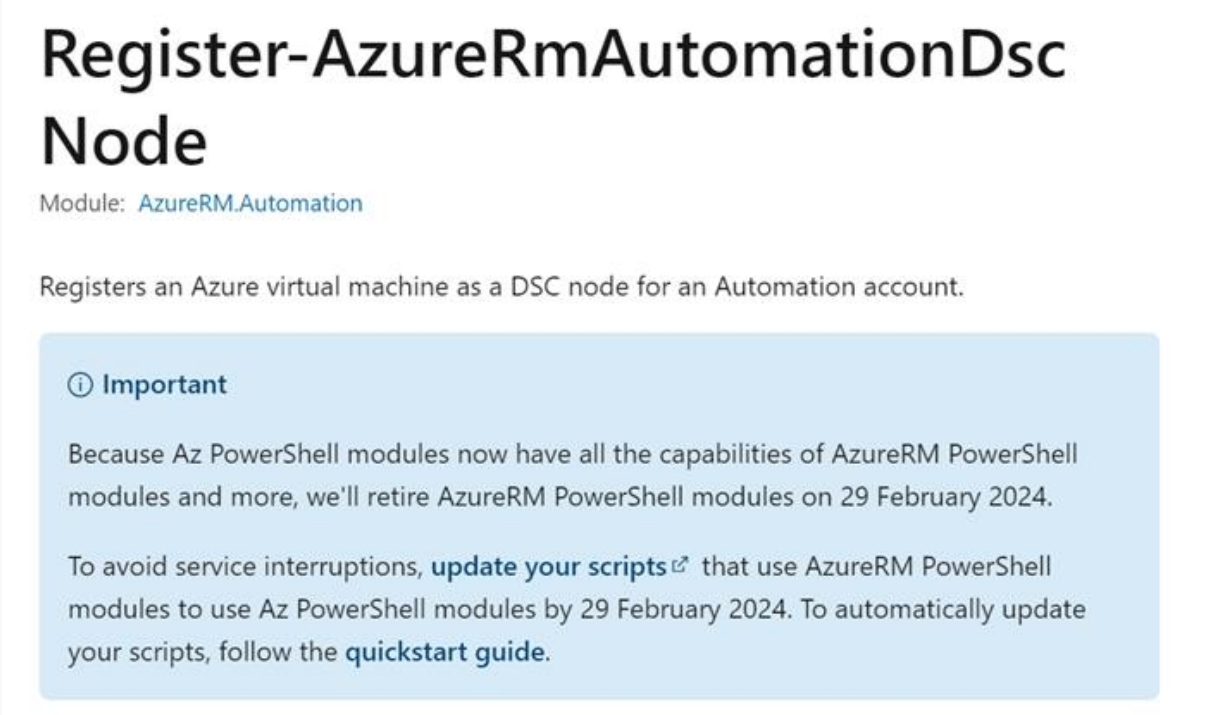
Question #8*Topic 1*

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 **Most Voted**

Hide Solution Discussion 7

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode?view=azurermps-6.13.0



Community vote distribution

B (100%)

Question #9*Topic 1*

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 **Most Voted**

Hide Solution | Discussion 10

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode?view=azurermps-6.13.0
Community vote distribution
B (100%)

Question #10*Topic 1*

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 **Most Voted**
- B. No

Hide Solution | Discussion 12

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode?view=azurermps-6.13.0
Community vote distribution
A (100%)

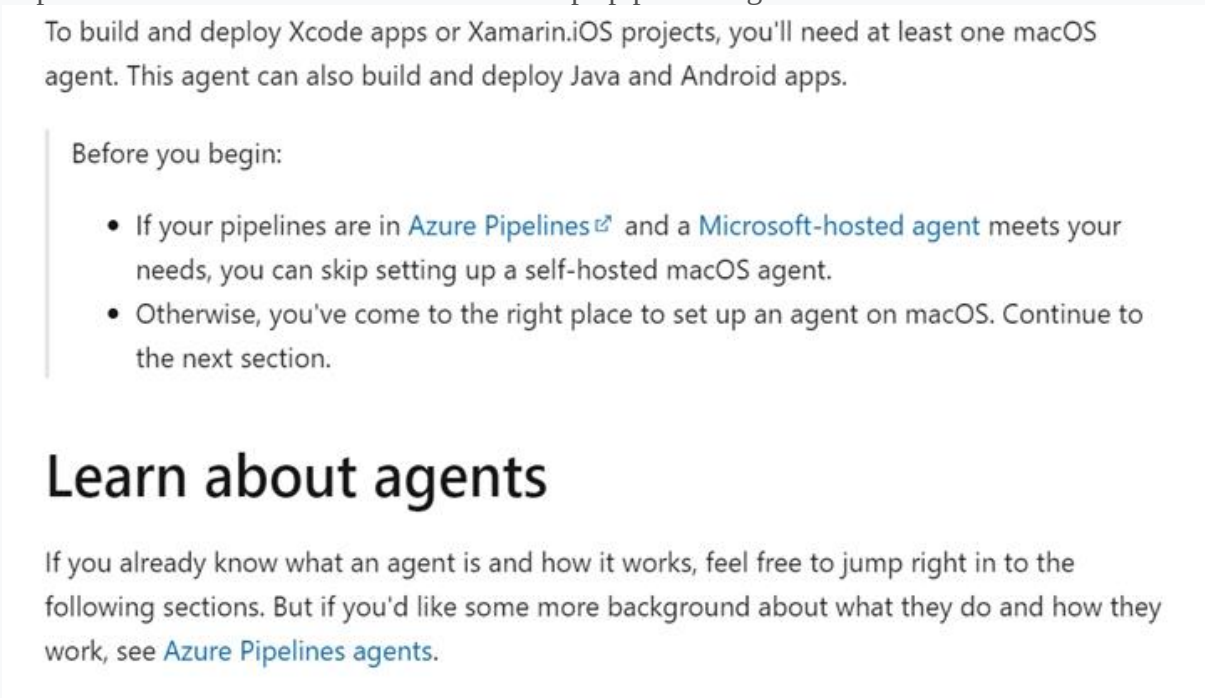
Question #11*Topic 1*

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 **Most Voted**
- C. Hosted **Most Voted**
- D. Hosted macOS

Hide Solution | Discussion 28

Correct Answer: *C*
Hosted pool (Azure Pipelines only): The Hosted pool is the built-in pool that is a collection of Microsoft-hosted agents.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-osx



Community vote distribution

B (58%)
C (42%)

Question #12*Topic 1*

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?

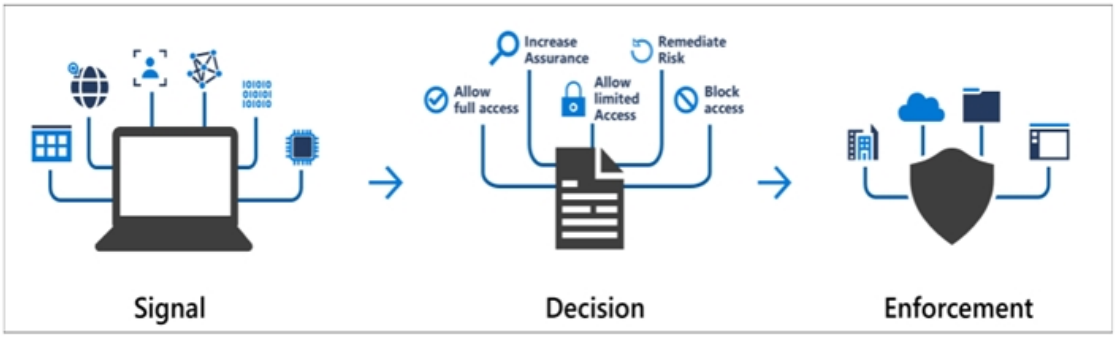
- A. Assign the devices to a security group.
- B. Create a GPO.
- C. Configure Security in Project Settings from Azure DevOps.
- D. Configure conditional access in Azure Active Directory. **Most Voted**

Hide Solution | Discussion 8

Correct Answer: *D*
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

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:

Community vote distribution

D (100%)

Question #13*Topic 1*

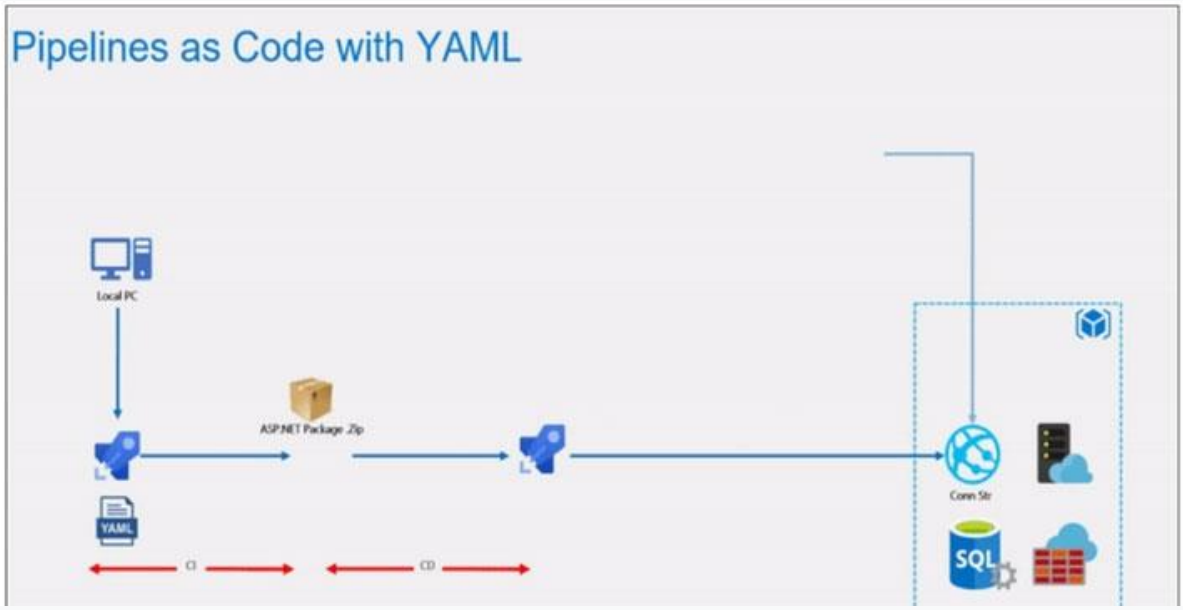
You are making use of Azure DevOps to configure Azure Pipelines for project, named PROJ-01.
You are preparing to use a version control system that allows for source code to be stored on a managed Windows server located on the company network.
Which of the following is the version control system you should use?

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

Hide Solution | Discussion 5

Correct Answer: *A*
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

Community vote distribution

A (100%)

Question #14*Topic 1*

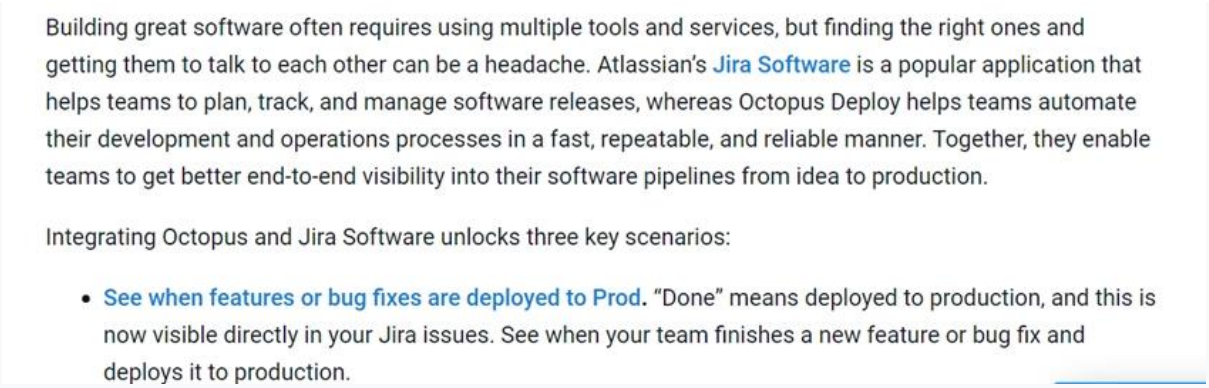
You need to consider the underlined segment to establish whether it is accurate.
When moving to Azure DevOps, JIRA must be replaced with the build pipelines Azure DevOps service.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the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

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

Hide Solution | Discussion 19

Correct Answer: *C*

Atlassian's Jira Software is a popular application that helps teams to plan, track, and manage software releases, whereas Octopus Deploy helps teams automate their development and operations processes in a fast, repeatable, and reliable manner. Together, they enable teams to get better end-to-end visibility into their software pipelines from idea to production.
Reference:
https://octopus.com/blog/octopus-jira-integration


Building great software often requires using multiple tools and services, but finding the right ones and getting them to talk to each other can be a headache. Atlassian's Jira Software is a popular application that helps teams to plan, track, and manage software releases, whereas Octopus Deploy helps teams automate their development and operations processes in a fast, repeatable, and reliable manner. Together, they enable teams to get better end-to-end visibility into their software pipelines from idea to production.

Integrating Octopus and Jira Software unlocks three key scenarios:

- See when features or bug fixes are deployed to Prod. "Done" means deployed to production, and this is now visible directly in your Jira issues. See when your team finishes a new feature or bug fix and deploys it to production.

https://www.azuredevopslabs.com/labs/vstsextend/jenkins/

Community vote distribution

D (93%)
8%

Question #15*Topic 1*

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 **Most Voted**
- D. npm update

Hide Solution | Discussion 10

Correct Answer: *C*
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

Community vote distribution

C (100%)

Question #16*Topic 1*

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 **Most Voted**
- B. Rolling deployment
- C. ‚€Big Bang‚€ deployment
- D. Canary deployment

Hide Solution | Discussion 11

Correct Answer: *A*
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.
Reference:
https://dev.to/mostlyjason/intro-to-deployment-strategies-blue-green-canary-and-more-3a3

Community vote distribution

A (91%)
9%

Question #17*Topic 1*

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. **Most Voted**
- D. You should make use of an approval check.

Hide Solution | Discussion 13

Correct Answer: *C*
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

Community vote distribution

C (100%)

Question #18*Topic 1*

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 **Most Voted**
- D. resource

Hide Solution Discussion 8

Correct Answer: *C*
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

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.

Community vote distribution

C (100%)

Question #19*Topic 1*

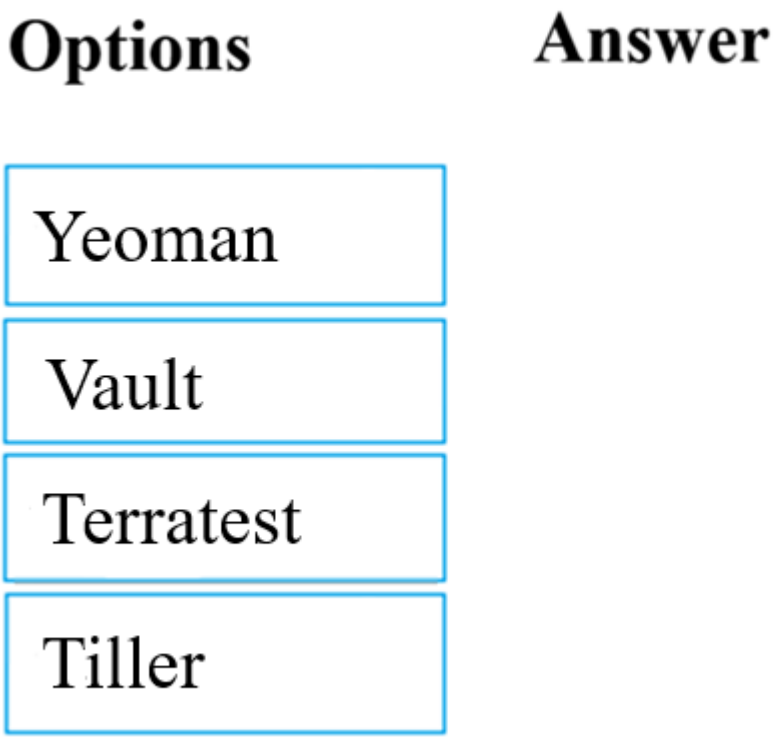
DRAG DROP -

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.

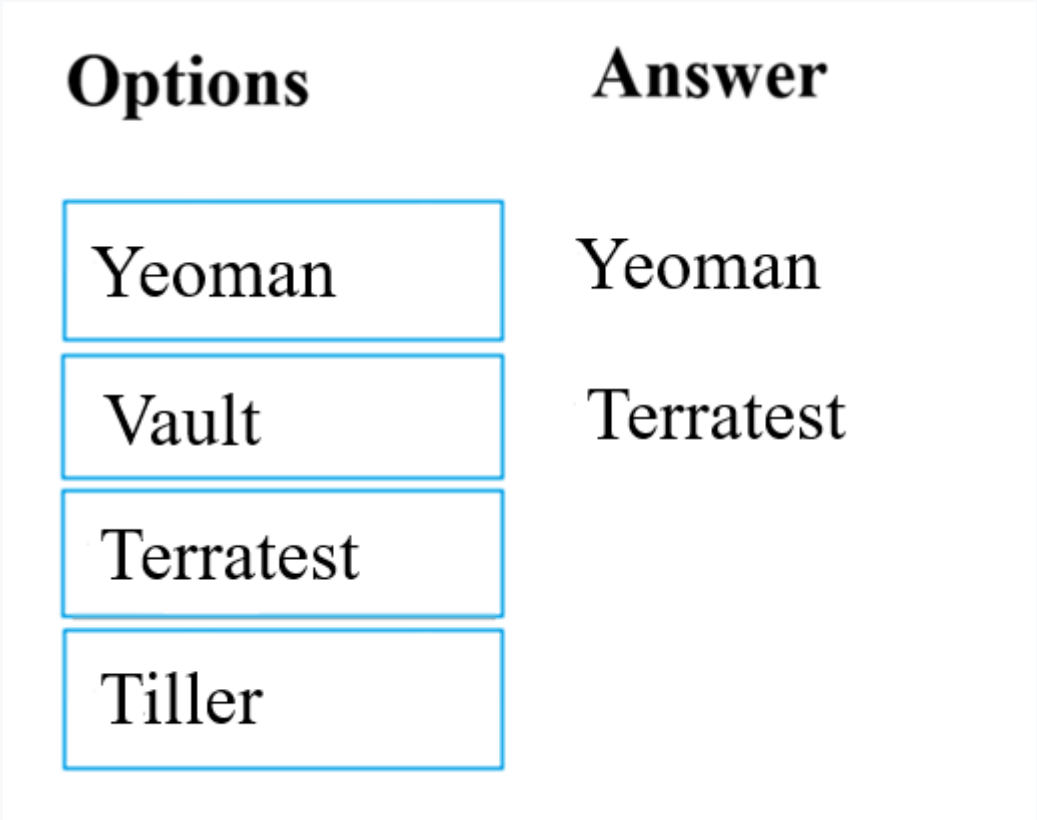
Select and Place:



Hide Solution Discussion 7

Correct

Answer:



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*Topic 1*

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. **Most Voted**
- C. You should make use of dynamic code analysis.
- D. You should make use of upstream sources.

Hide Solution | Discussion 21

Correct Answer: *D*
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
Reference:

https://docs.microsoft.com/en-us/azure/devops/artifacts/concepts/upstream-sources?view=vsts

Community vote distribution

B (100%)

Previous QuestionsNext Questions

Question #21*Topic 1*

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 **Most Voted**
- D. OWASP ZAP

Hide Solution Discussion 8

Correct Answer: *C*

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/

Community vote distribution

C (100%)

Question #22*Topic 1*

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. **Most Voted**
- 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.

Hide Solution Discussion 9

Correct Answer: *A*
Reference:
https://www.azuredevopslabs.com/labs/vstsextend/whitesource/
Community vote distribution
A (100%)

Question #23*Topic 1*
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. **Most Voted**
- B. Maven
- C. Bamboo
- D. CMAKE

Hide Solution Discussion 8

Correct Answer: *A*
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
Community vote distribution
A (100%)

Question #24*Topic 1*
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 **Most Voted**
- B. The PowerShell Desired State Configuration (DSC) extension for Windows **Most Voted**
- C. Azure pipeline deployment groups
- D. The Custom Script Extension for Windows
- E. Azure pipeline stage templates

Hide Solution Discussion 30

Correct Answer: *AD*
The Custom Script Extension downloads and executes scripts on Azure virtual machines. This extension is useful for post deployment configuration, software installation, or any other configuration or management tasks. Scripts can be downloaded from Azure storage or GitHub, or provided to the Azure portal at extension run time. The Custom Script Extension integrates with Azure Resource Manager templates, and can be run using the Azure CLI, PowerShell, Azure portal, or the Azure Virtual Machine REST API.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/custom-script-windows
Community vote distribution

AB (81%)
Other

Question #25*Topic 1*

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 **Most Voted**

Hide Solution | Discussion 11

Correct Answer: *D*
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:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-diagnostics
Community vote distribution

D (100%)

Question #26*Topic 1*

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 **Most Voted**
- C. Azure Log Analytics
- D. Azure Advisor

Hide Solution Discussion 8

Correct Answer: *B*
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
Community vote distribution
B (100%)

Question #27*Topic 1*
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 **Most Voted**

Hide Solution Discussion 10

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-sql
Community vote distribution
B (100%)

Question #28*Topic 1*
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 **Most Voted**

Hide Solution Discussion 9

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-sql
Community vote distribution
B (100%)

Question #29*Topic 1*

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 **Most Voted**
- B. No **Most Voted**

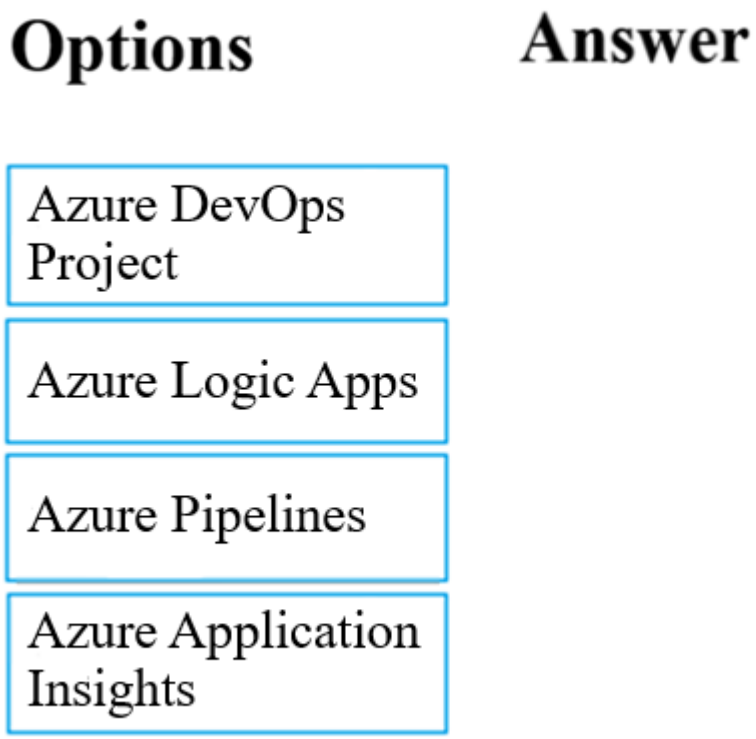
Hide Solution | Discussion 48

Correct Answer: *B*
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
Community vote distribution
B (60%)
A (40%)

Question #30*Topic 1*

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:



Hide Solution Discussion 8

Question #31*Topic 1*

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. **Most Voted**
- B. OWASP ZAP
- C. TFS Integration Platform
- D. Code Style

Hide Solution Discussion 10

Correct Answer: *A*
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

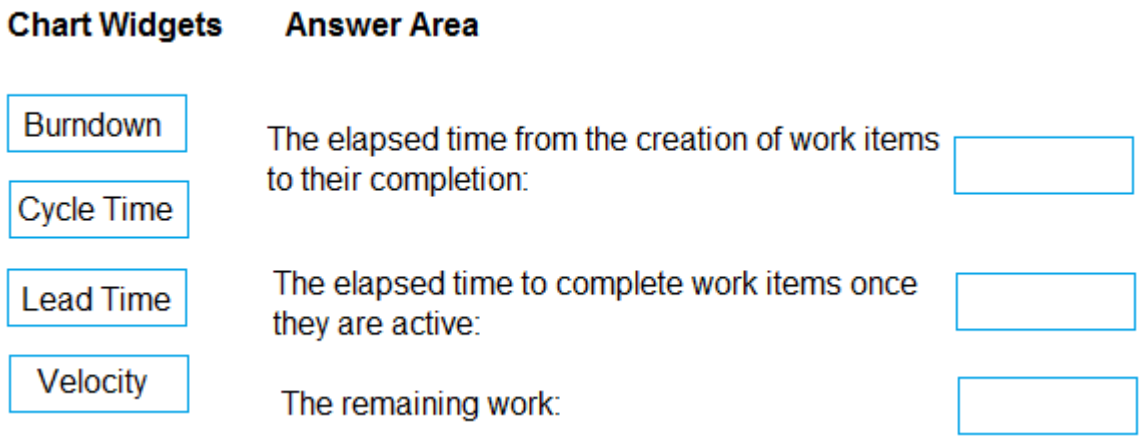
the pipeline and will be enabled once Edge moves to a Chromium- compatible web platform.
Reference:
https://marketplace.visualstudio.com/items?itemName=ms.vss-exploratorytesting-web
Community vote distribution

A (100%)

2 Topic 2 - Question Set 2

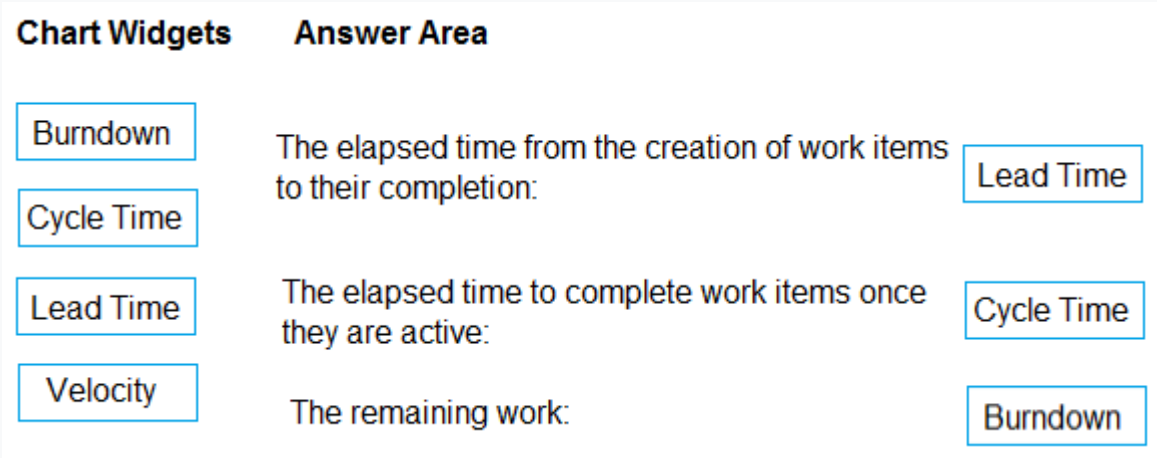
Question #1*Topic 2*

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:



Hide Solution | Discussion 26

Correct Answer:



Box 1: Lead time -
Lead time measures the total time elapsed from the creation of work items to their completion.

Box 2: Cycle time -

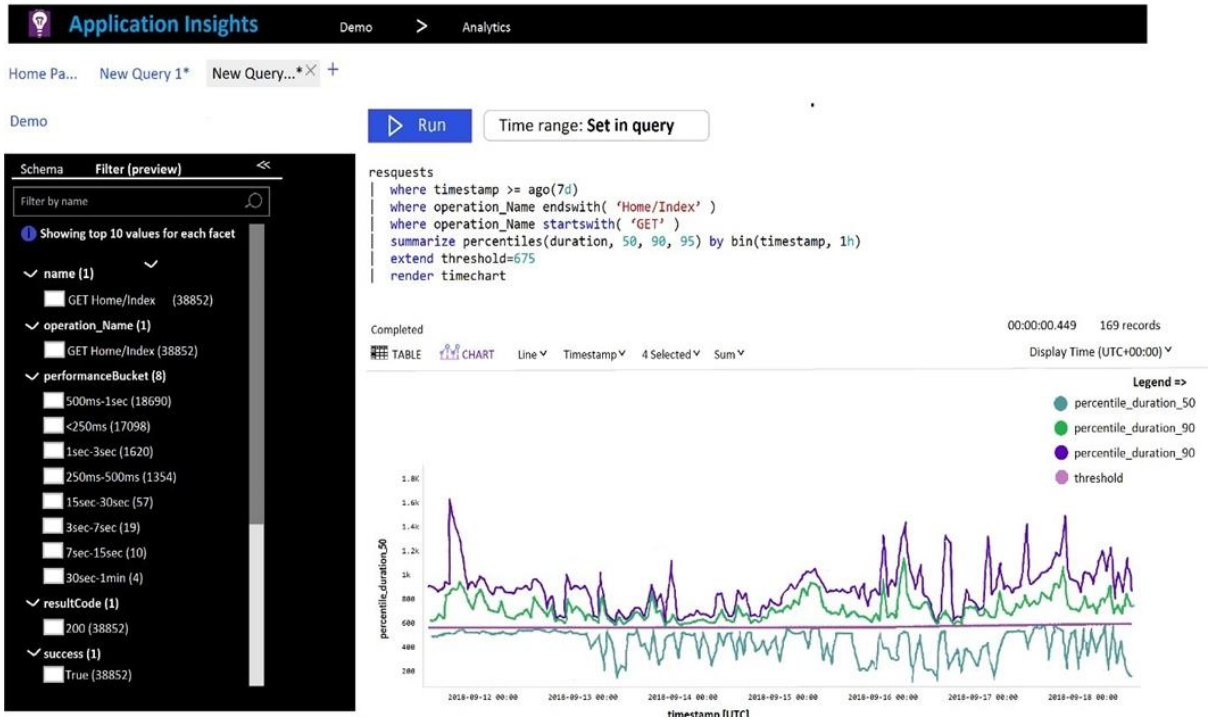
Cycle time measures the time it takes for your team to complete work items once they begin actively working on them.

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 #2*Topic 2*

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.



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

Hide Solution | Discussion 44

Correct 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**

Box 1: percentile_duration_95 -

Box 2: success -
For example ‚€"
requests
| project name, url, success
| where success == "False"
This will return all the failed requests in my App Insights within the specified time range.
Reference:
https://devblogs.microsoft.com/premier-developer/alerts-based-on-analytics-query-using-custom-log-search/

Question #3*Topic 2*

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 **Most Voted**
- B. an Azure Monitor alert that has a dynamic threshold **Most Voted**
- 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

Hide Solution | Discussion 17

Correct Answer: *AB*

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

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

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-dynamic-thresholds
https://docs.microsoft.com/en-us/azure/automation/automation-create-alert-triggered-runbook

Community vote distribution

AB (100%)

Question #4*Topic 2*

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]

Hide Solution | Discussion 25

Correct 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:
readinessProbe:
ShutdownProbe:
startupProbe:

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

initialDelaySeconds: 15
periodSeconds: 15
timeoutSeconds: 15

Box 1: readinessProbe:
For containerized applications that serve traffic, you might want to verify that your container is ready to handle incoming requests. Azure Container Instances supports readiness probes to include configurations so that your container can't be accessed under certain conditions.
Incorrect Answers:
livenessProbe: 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.

Box 2: periodSeconds: 15 -
The periodSeconds property designates the readiness command should execute every 15 seconds.
Reference:
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-readiness-probe

Question #5*Topic 2*

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. **Most Voted**
- C. Write an Azure function and deploy the function to the specific regions.
- D. Create an Azure Service Health alert for the specific regions.

Hide Solution | Discussion 20

Correct Answer: *B*
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
Community vote distribution
B (100%)

Question #6*Topic 2*

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 **Most Voted**
- B. the activity log of the App Service
- C. the diagnostics logs of the App Service
- D. Azure Advisor

Hide Solution | Discussion 18

Correct Answer: *A*
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

Community vote distribution

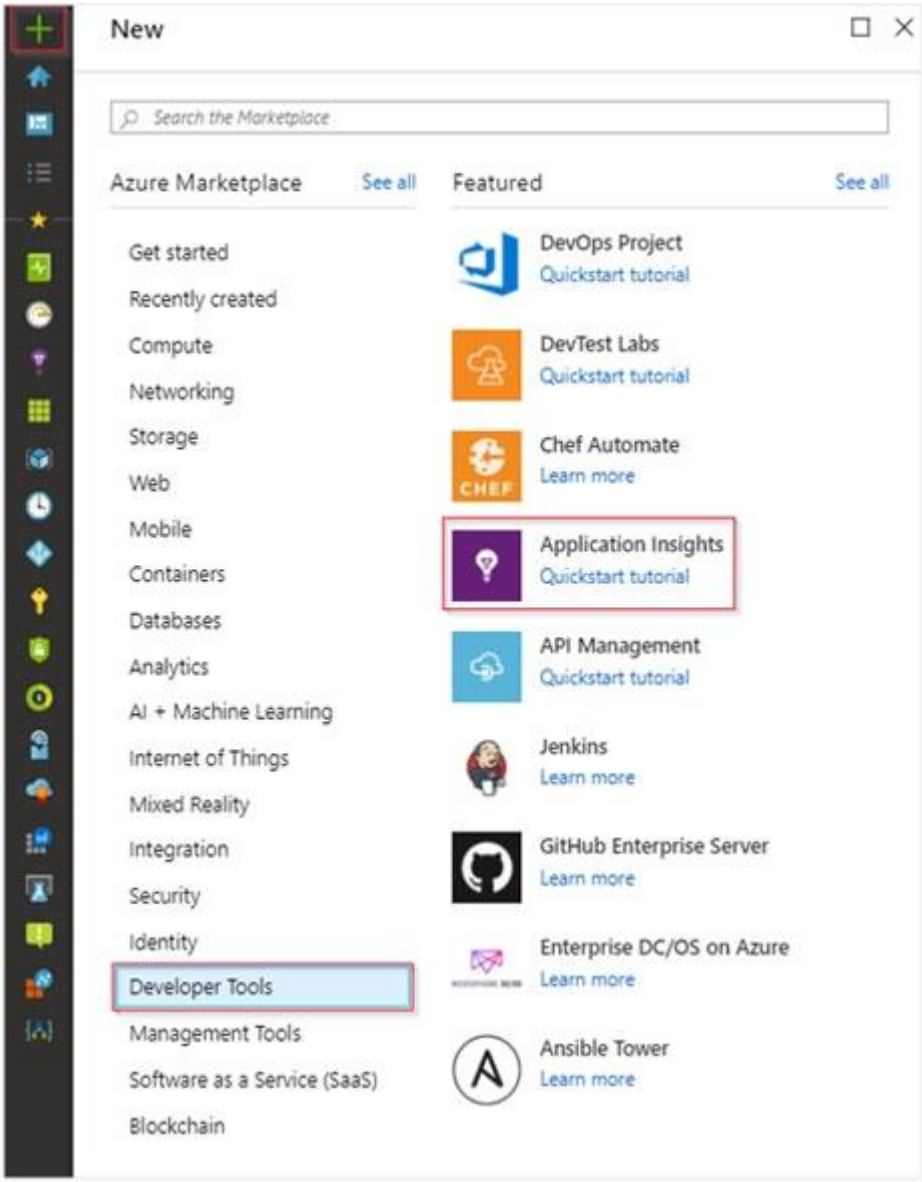
A (100%)

Question #7*Topic 2*

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.

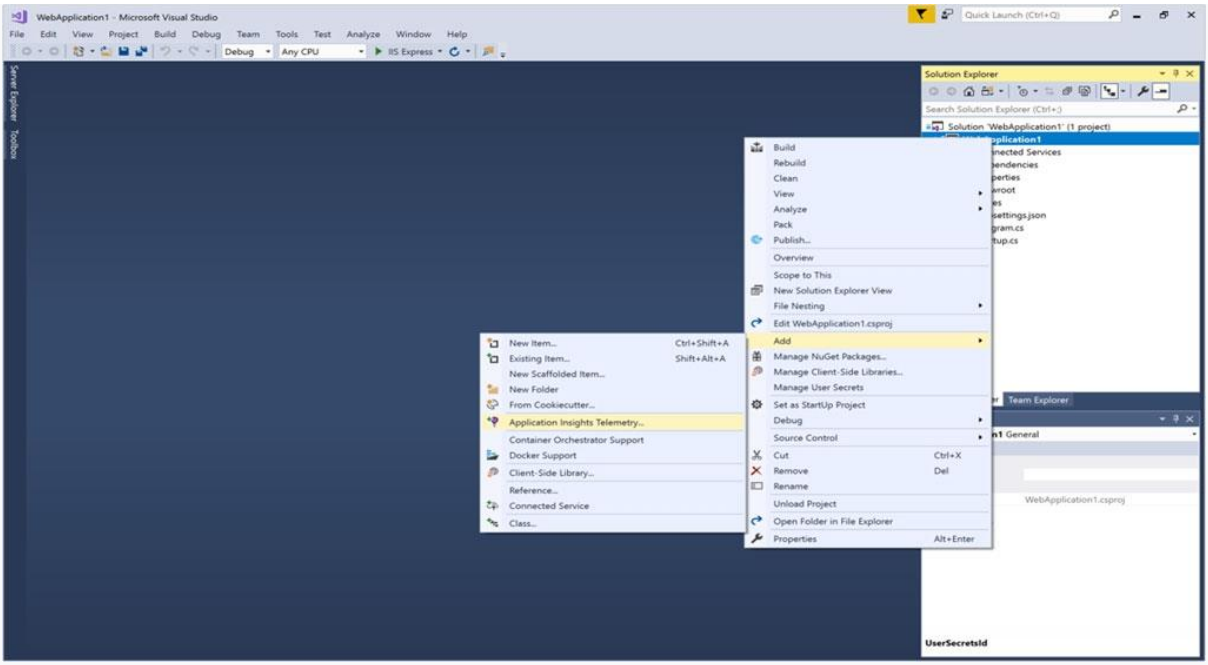
Hide Solution | Discussion 3

Correct Answer: *See explanation below.*
Step 1: Create an instance of Azure Application Insights
1. Open Microsoft Azure Portal
2. Log into your Azure account, Select Create a resource > Developer tools > Application Insights.



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

Name: az400-123456789-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 #8*Topic 2*

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) **Most Voted**
- D. Insight & Analytics

Hide Solution | Discussion 11

Correct Answer: *C*

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 -

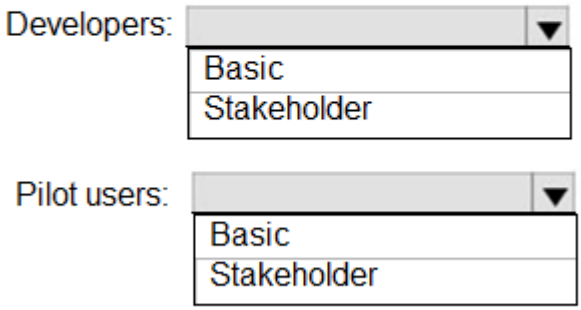
☞ Create work items in ITSM tool, based on your Azure alerts (metric alerts, Activity Log alerts and Log Analytics alerts).
☞ Optionally, you can sync your incident and change request data from your ITSM tool to an Azure Log Analytics workspace.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/itsmc-overview
Community vote distribution

C (100%)

Question #9*Topic 2*

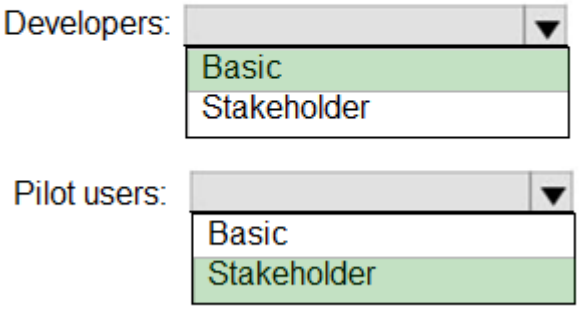
HOTSPOT -
Your company is building a new web application.
You plan to collect feedback from pilot users on the features being delivered.
All the pilot users have a corporate computer that has Google Chrome and the Microsoft Test & Feedback extension installed. The pilot users will test the application 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



Hide Solution Discussion 31

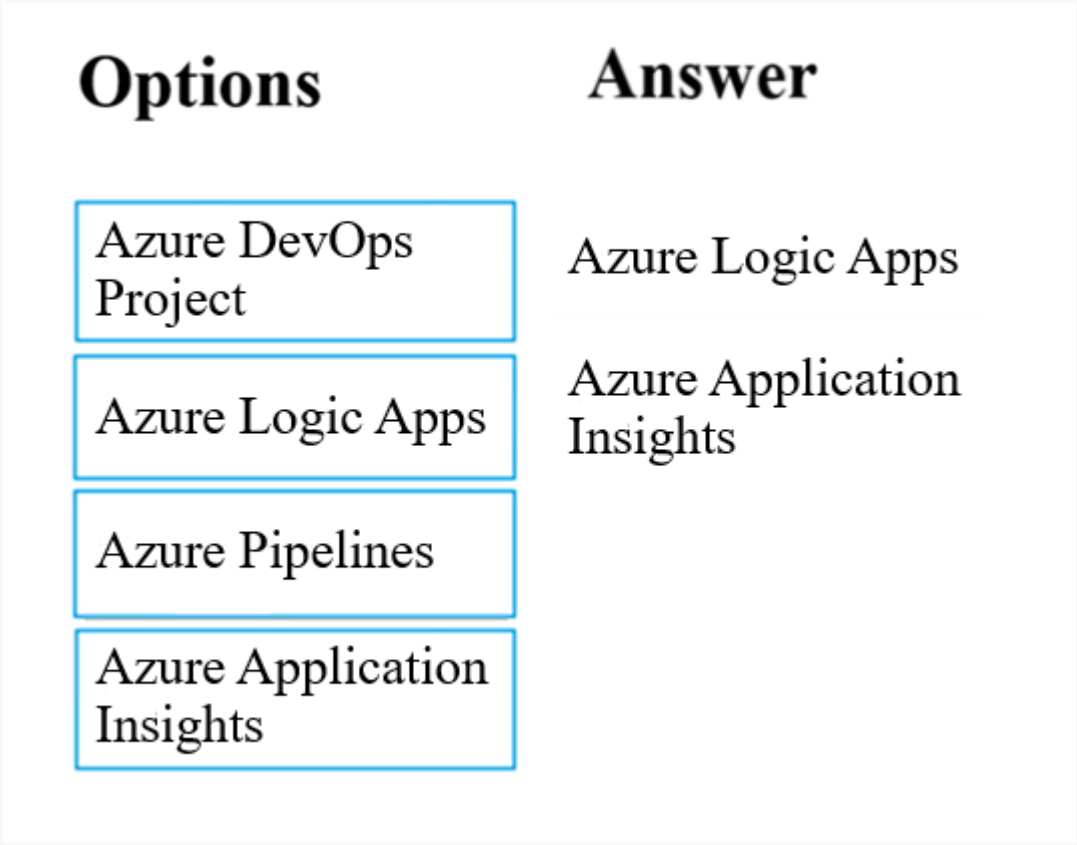
Answer Area



Correct Answer:
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

Correct



Answer:

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 #10*Topic 2*

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) **Most Voted**
- B. PL/pgSQL

- C. PL/SQL
- D. Transact-SQL

Hide Solution Discussion 13

Correct Answer: *A*
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
Community vote distribution
A (100%)

Question #11*Topic 2*

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 **Most Voted**
- B. Azure Pipelines
- C. Microsoft Visual Studio App Center
- D. Azure DevOps Project
- E. Azure Application Insights **Most Voted**

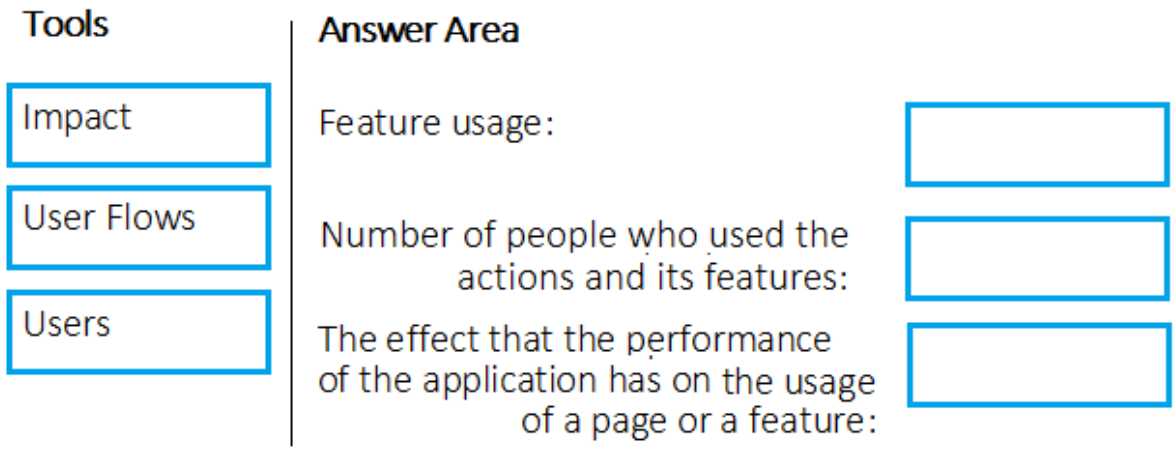
Hide Solution Discussion 17

Correct Answer: *AE*
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
Community vote distribution
AE (100%)

Question #12*Topic 2*

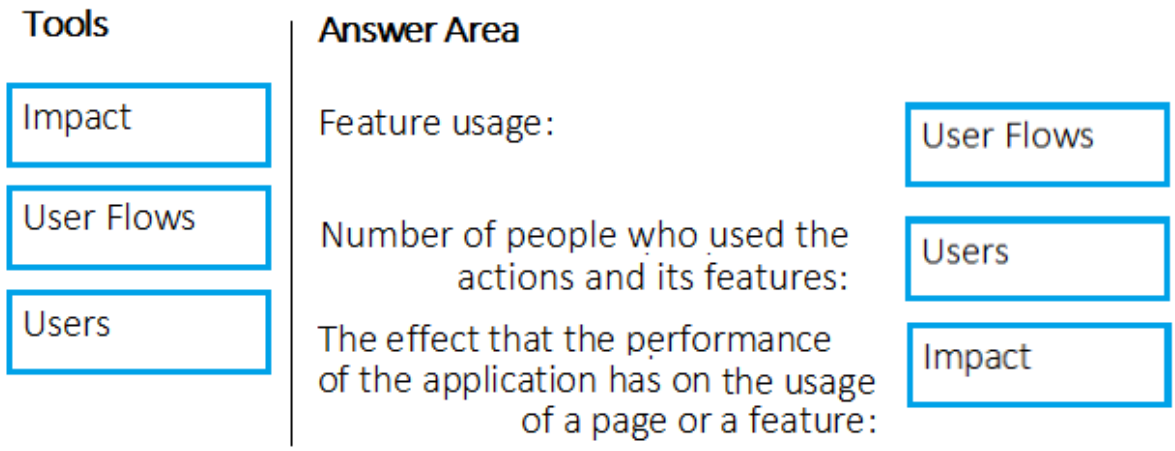
DRAG DROP -
Your company wants to use Azure Application Insights to understand how user behaviors affect an application.

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



Hide Solution Discussion 34

Correct Answer:



Box 1: User Flows -
The User Flows tool visualizes how users navigate between the pages and features of your site. It's great for answering questions like:
How do users navigate away from a page on your site?
What do users click on a page on your site?
Where are the places that users churn most from your site?
Are there places where users repeat the same action over and over?

Box 2: Users -
Counting Users: The user behavior analytics tools don't currently support counting users or sessions based on properties other than anonymous user ID, authenticated user ID, or session ID.

Box 3: Impact -
Impact analyzes how load times and other properties influence conversion rates for various parts of your app. To put it more precisely, it discovers how any dimension of a page view, custom event, or request affects the usage of a different page view or custom event.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-flows
https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-impact
https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-troubleshoot

Question #13*Topic 2*

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 **Most Voted**
- C. Azure Application Insights widgets
- D. Jenkins integration

Hide Solution | Discussion 52

Correct Answer: *A*
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
Community vote distribution
B (100%)

Question #14*Topic 2*

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. **Most Voted**
- D. Modify the Custom Script extension settings of VMSS1. **Most Voted**
- E. Update the configuration of a virtual machine in VMSS1. **Most Voted**

Hide Solution | Discussion 32

Correct Answer: *BCD*

Community vote distribution

CDE (100%)

Question #15*Topic 2*

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.

Hide Solution | Discussion 3

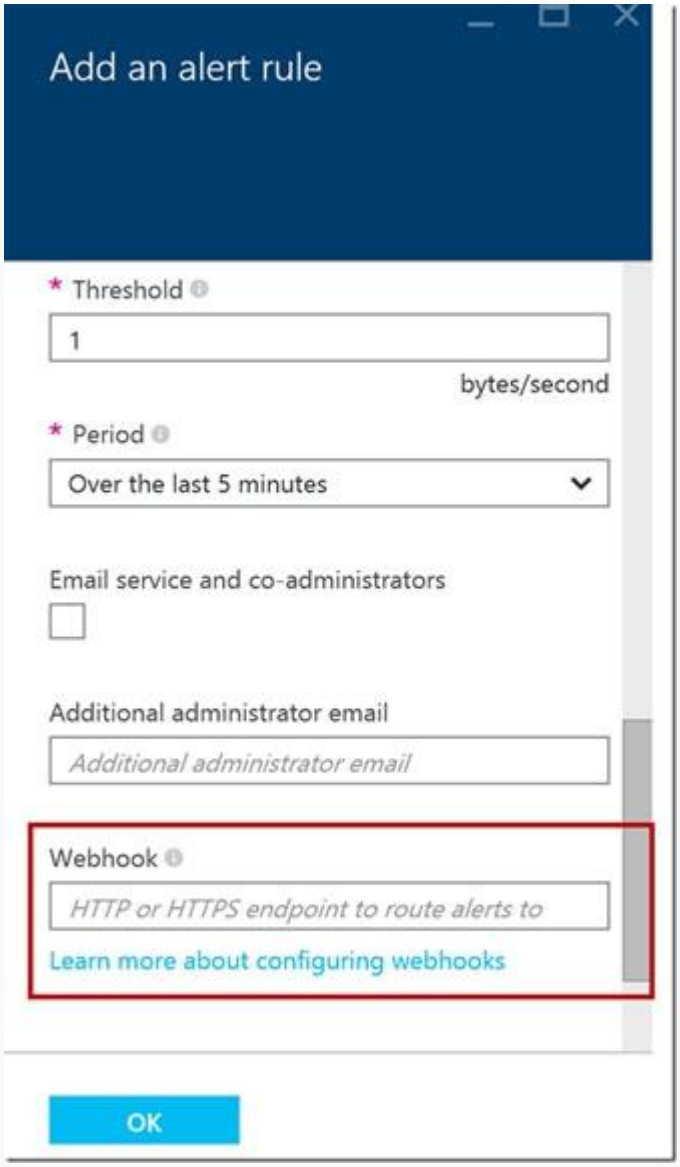
Correct Answer: *See explanation below.*
1. Open Microsoft Azure Portal
2. Log into your Azure account and go to App Service and look under Monitoring then you will see Alert.
3. Select Add an alert rule
4. Configure the alert rule as per below and click Ok.

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

Question #16*Topic 2*

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.

Hide Solution | Discussion 1

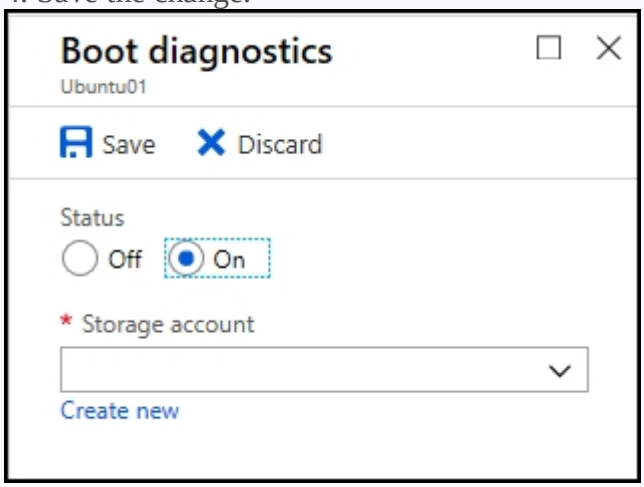
Correct Answer: *See explanation below.*
Step 1: To create a general-purpose v2 storage account in the Azure portal, follow these steps:
1. On the Azure portal menu, select All services. In the list of resources, type Storage Accounts. As you begin typing, the list filters based on your input. Select 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 #17*Topic 2*

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.

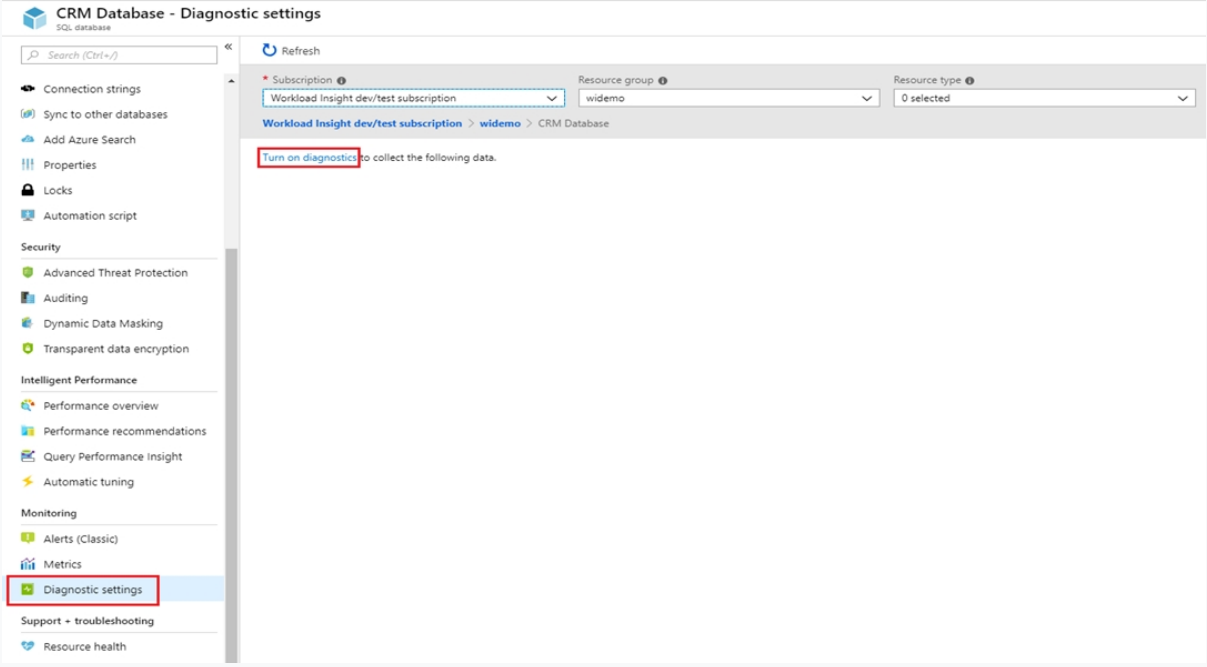
To complete this task, sign in to the Microsoft Azure portal.

Hide Solution | Discussion 9

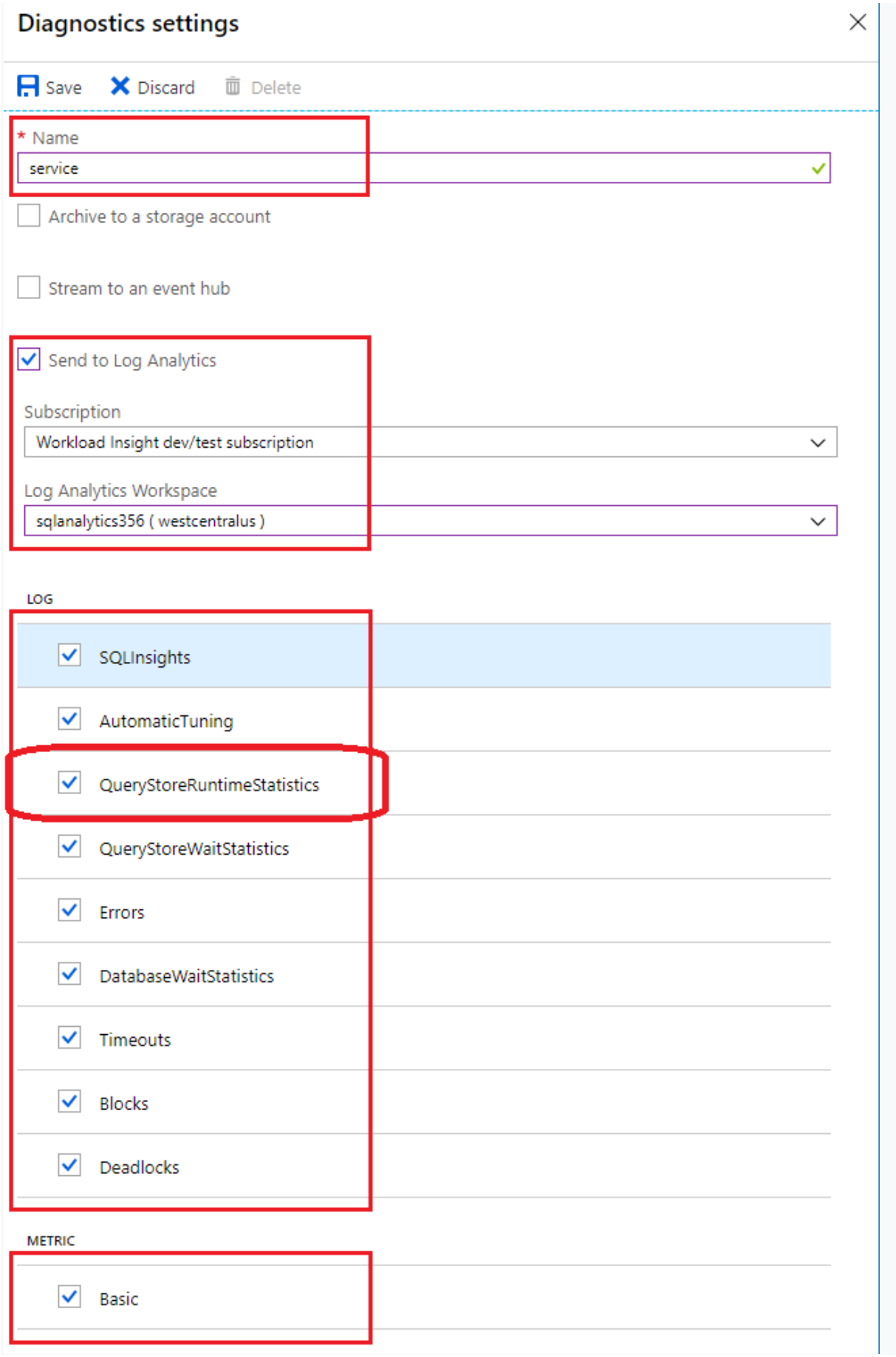
Correct Answer: *See explanation below.*

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

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



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


Diagnostics settings
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 #18*Topic 2*

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

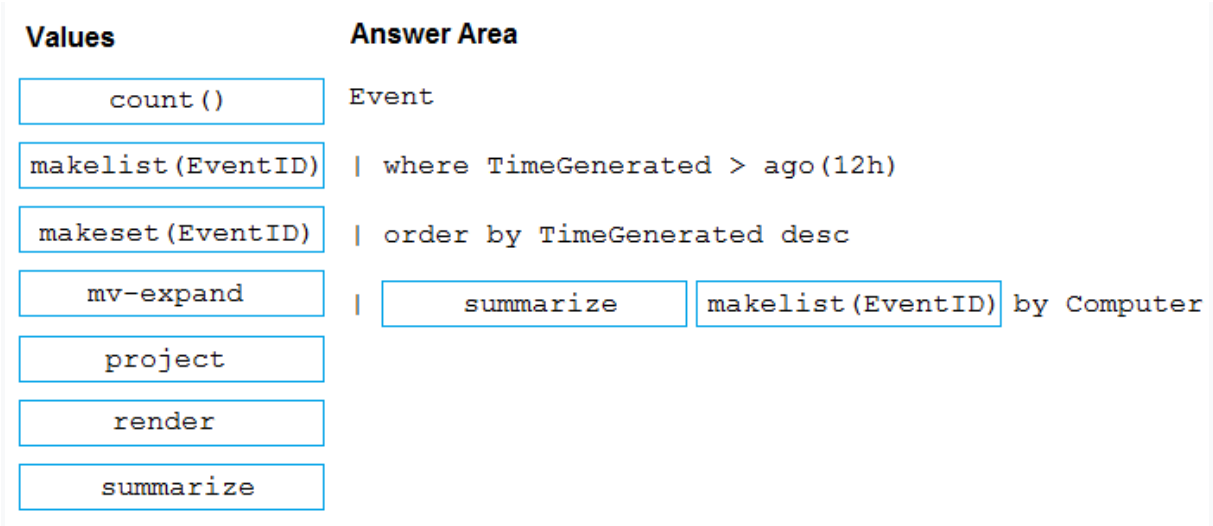
- count()
- makelist(EventID)
- makeset(EventID)
- mv-expand
- project
- render
- summarize

Answer Area

```
Event
| where TimeGenerated > ago(12h)
| order by TimeGenerated desc
| [ ] [ ] by Computer
```

Hide Solution Discussion 30

Correct Answer:



You can use makelist to pivot data by the order of values in a particular column. For example, you may want to explore the most common order events take place on your machines. You can essentially pivot the data by the order of EventIDs on each machine.
Example:

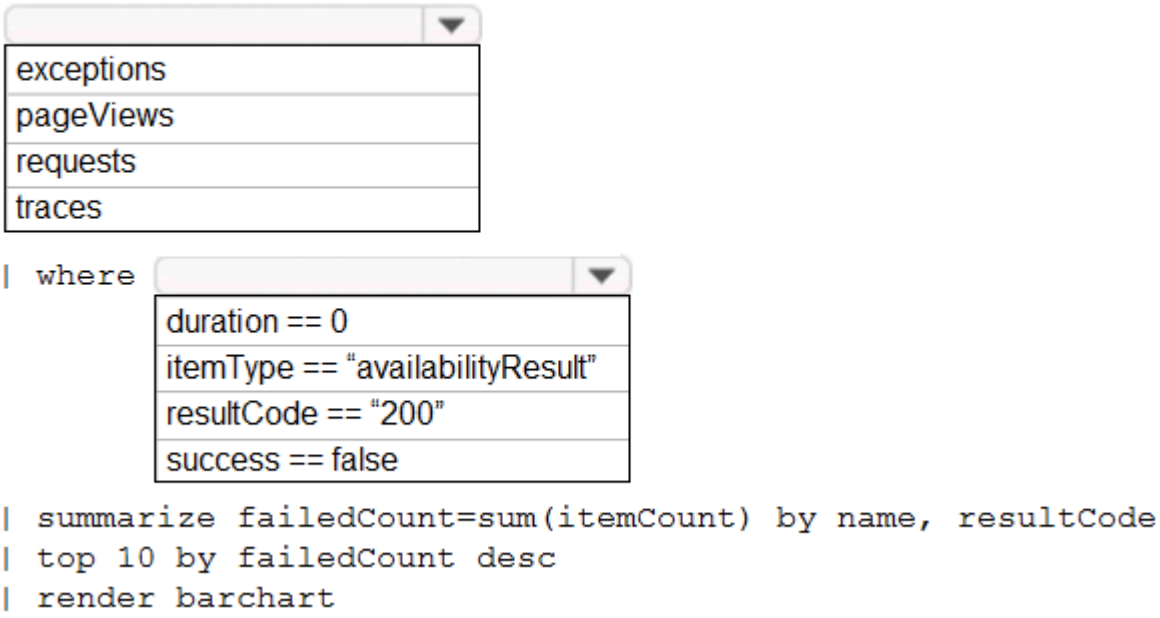
Event -
| where TimeGenerated > ago(12h)
| order by TimeGenerated desc
| summarize makelist(EventID) by Computer
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/advanced-aggregations

Question #19*Topic 2*

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:

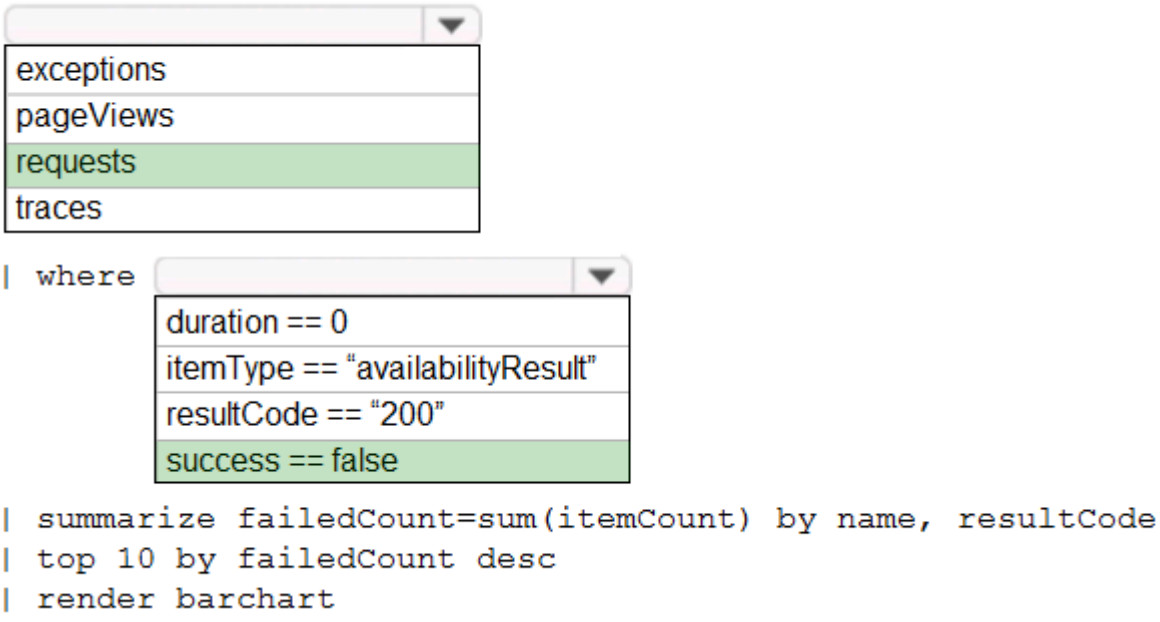
Answer Area



Hide Solution Discussion 15

Correct Answer:

Answer Area



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 #20*Topic 2*

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 **Most Voted**
- E. Continuous export

Hide Solution | Discussion 15

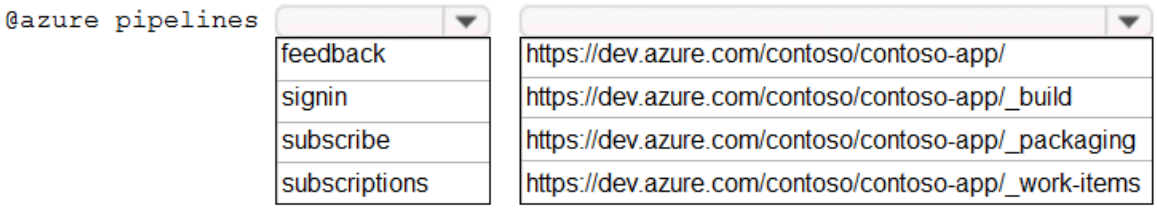
Correct Answer: *D*
Smart Detection automatically warns you of potential performance problems and failure anomalies in your web application. It performs proactive analysis of the telemetry that your app sends to Application Insights. If there is a sudden rise in failure rates, or abnormal patterns in client or server performance, you get an alert.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-diagnostics
Community vote distribution
D (100%)

Question #21*Topic 2*

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:

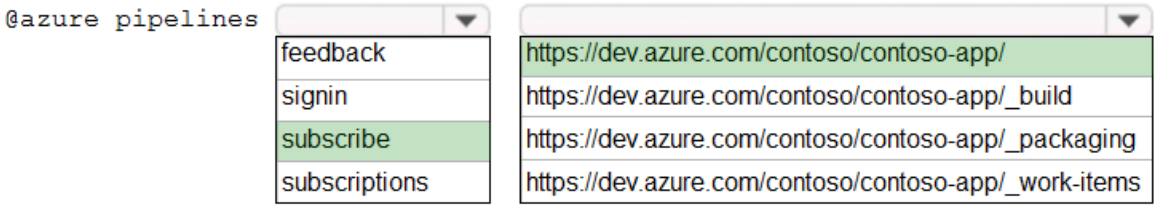
Answer Area



Hide Solution Discussion 26

Correct Answer:

Answer Area



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]

Question #22*Topic 2*

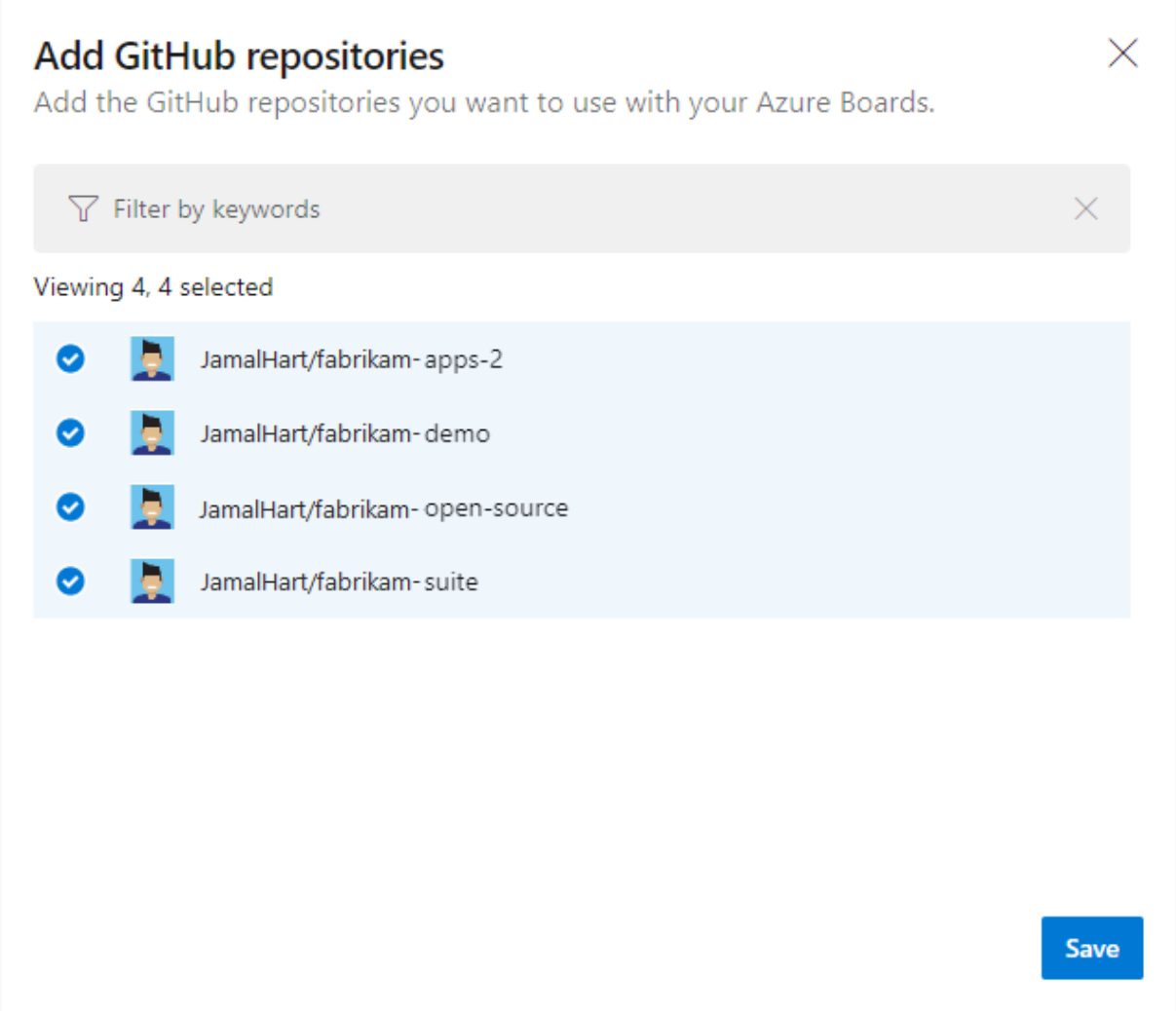
You have a private GitHub repository.
You need to display the commit status of the repository on Azure Boards.
What should you do first?

- 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. **Most Voted**
- D. Create a GitHub action in GitHub.

Hide Solution Discussion 14

Correct Answer: *C*
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.



Reference:
https://docs.microsoft.com/en-us/azure/devops/boards/github/connect-to-github

Community vote distribution

C (100%)

Question #23*Topic 2*

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. **Most Voted**
- D. From Azure Pipelines, enable continuous integration for Project1.

Hide Solution | Discussion 60

Correct Answer: *A*

To start monitoring all pipelines in a project, use the following command inside a channel:
@azure pipelines subscribe [project url]
The project URL can be to any page within your project (except URLs to pipelines).
For example:
@azure pipelines subscribe https://dev.azure.com/myorg/myproject/
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams

Community vote distribution

C (90%)
10%

Question #24*Topic 2*

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

Hide Solution | Discussion 44

Correct Answer: *A*

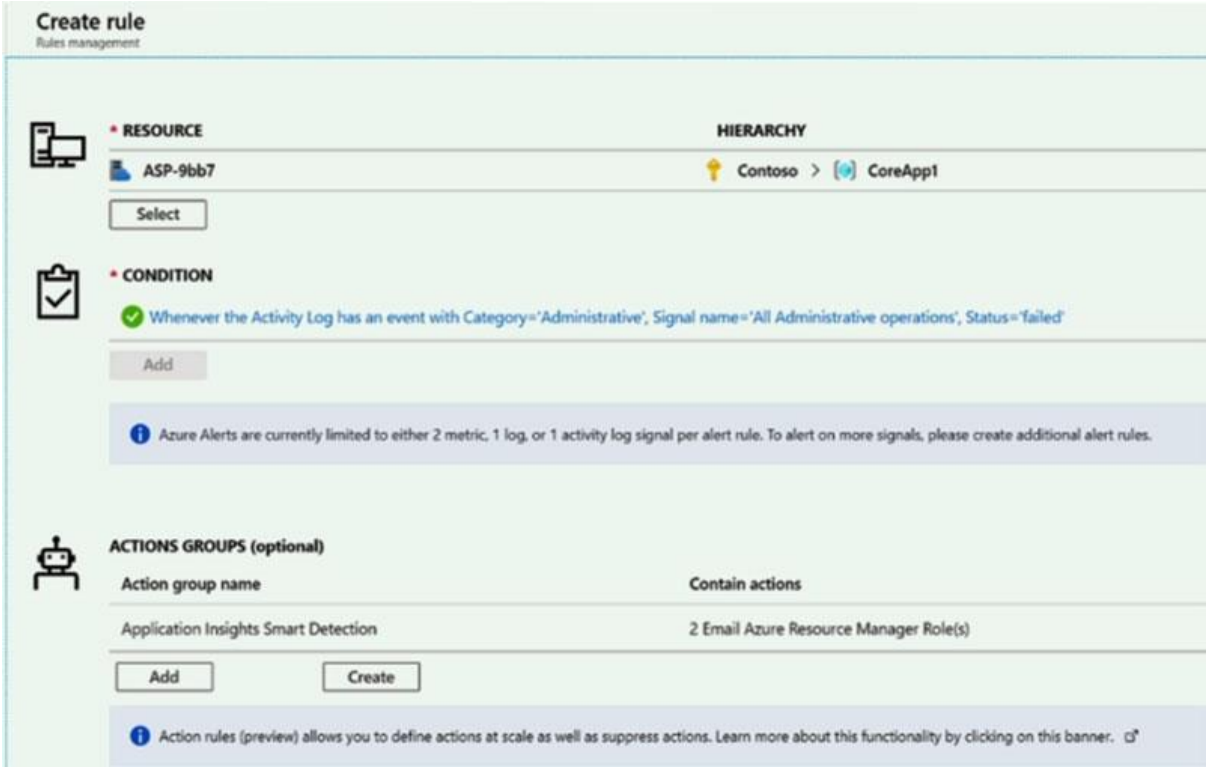
Service hooks let you run tasks on other services when events happen in your Azure DevOps projects. For example, create a card in Trello when a work item is created or send a push notification to your team's mobile devices when a build fails. You can also use service hooks in custom apps and services as a more efficient way to drive activities when events happen in your projects.
Note: Service hook publishers define a set of events. Subscriptions listen for the events and define actions to take based on the event. Subscriptions also target consumers, which are external services that can run their own actions, when an event occurs.
Reference:
https://docs.microsoft.com/en-us/azure/devops/service-hooks/overview

Community vote distribution

B (80%)
10%
10%

Question #25*Topic 2*

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



Which action will trigger an alert?

- A. a failed attempt to delete the ASP-9bb7 resource **Most Voted**
- 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

Hide Solution | Discussion 16

Correct Answer: *A*

Community vote distribution

A (100%)

Question #26*Topic 2*

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 **Most Voted**
- B. Stream to an event hub
- C. Archive to a storage account

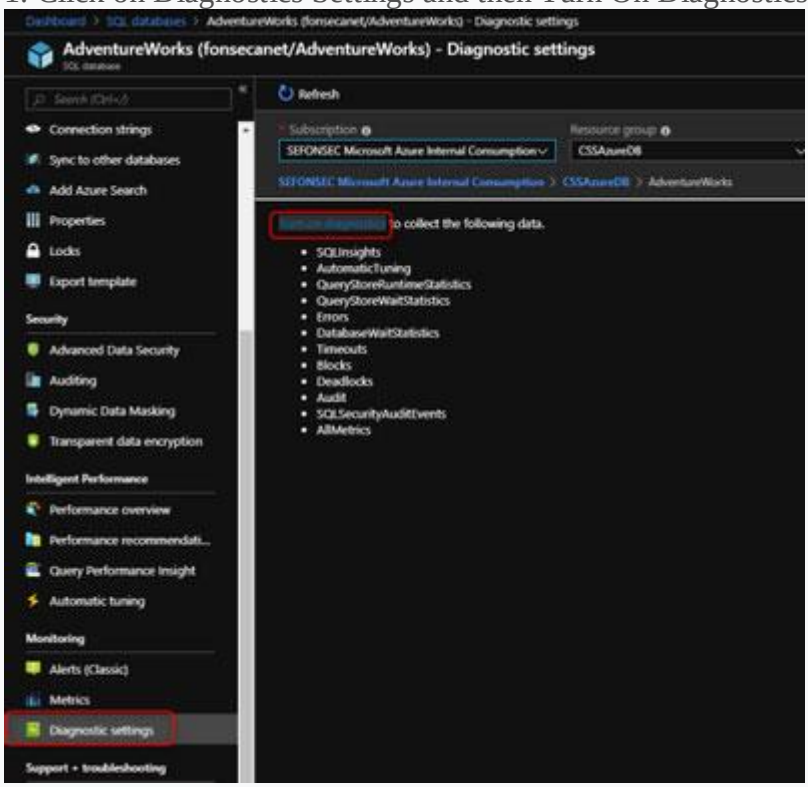
Hide Solution | Discussion 11

Correct Answer: *A*

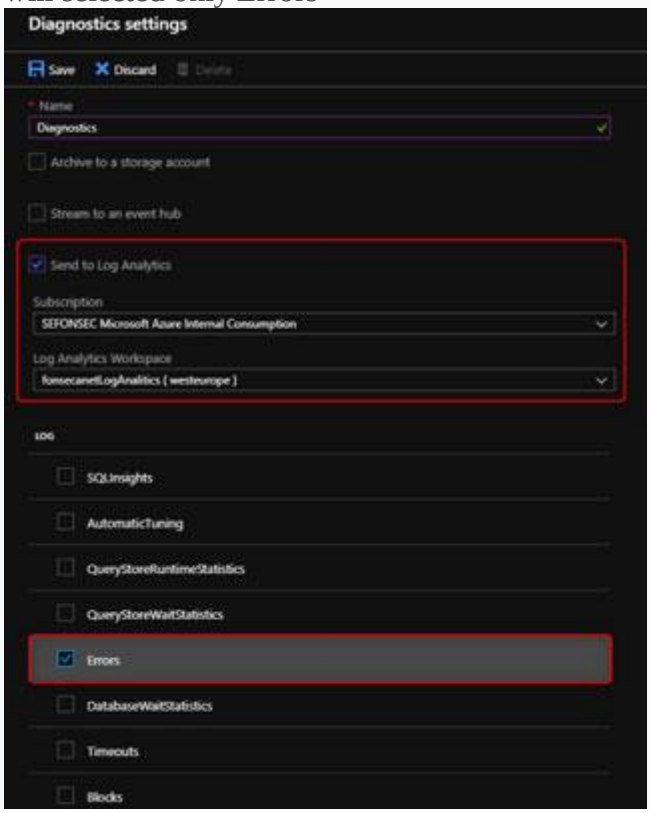
ENABLE DIAGNOSTICS TO LOG ANALYTICS

This configuration is done PER DATABASE

1. Click on Diagnostics Settings and then Turn On Diagnostics



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



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

Community vote distribution

A (100%)

Question #27*Topic 2*

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.

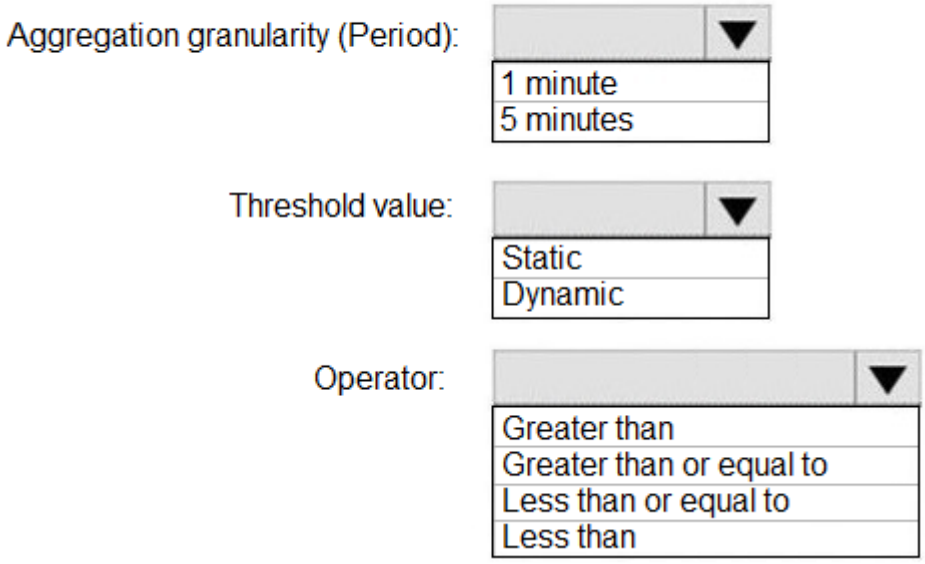
The alert must calculate the average once every minute.

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:

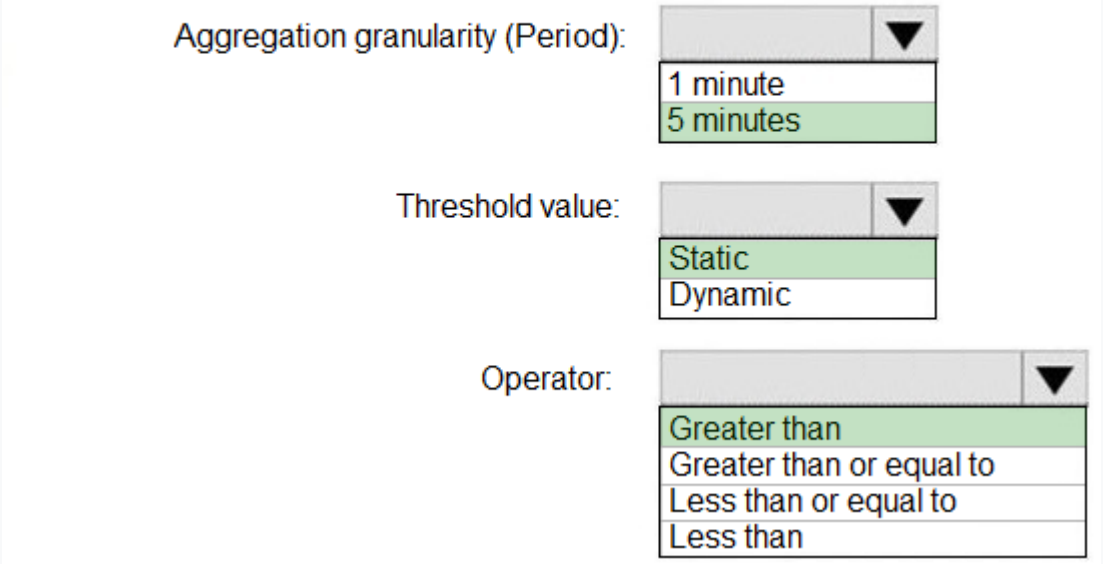
Answer Area



Hide Solution | Discussion 17

Correct Answer:

Answer Area



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

Question #28*Topic 2*

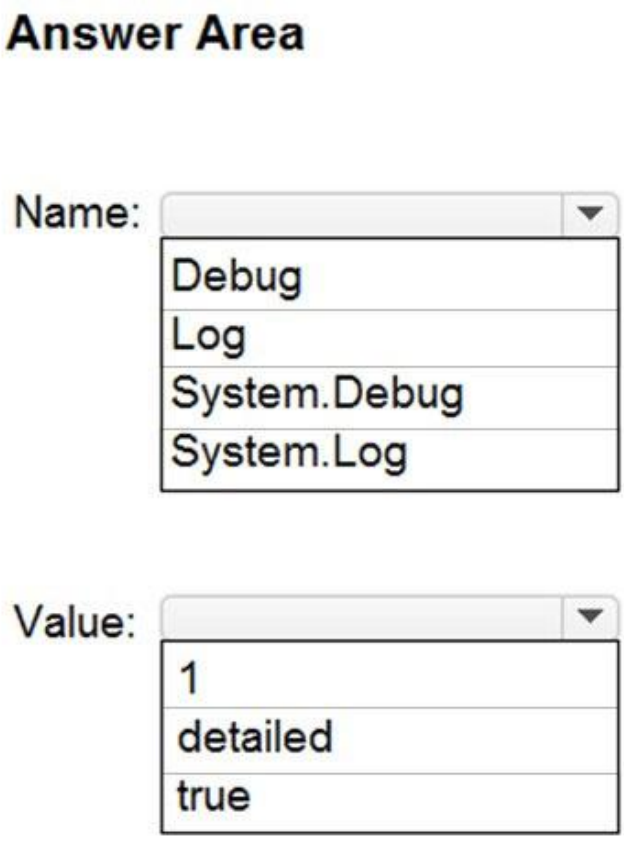
You have an Azure virtual machine that is monitored by using Azure Monitor.
The virtual machine has the Azure Log Analytics agent installed.
You plan to deploy the Service Map solution from the Azure Marketplace.
What should you deploy to the virtual machine to support the Service Map solution?

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

Reveal Solution Discussion 8

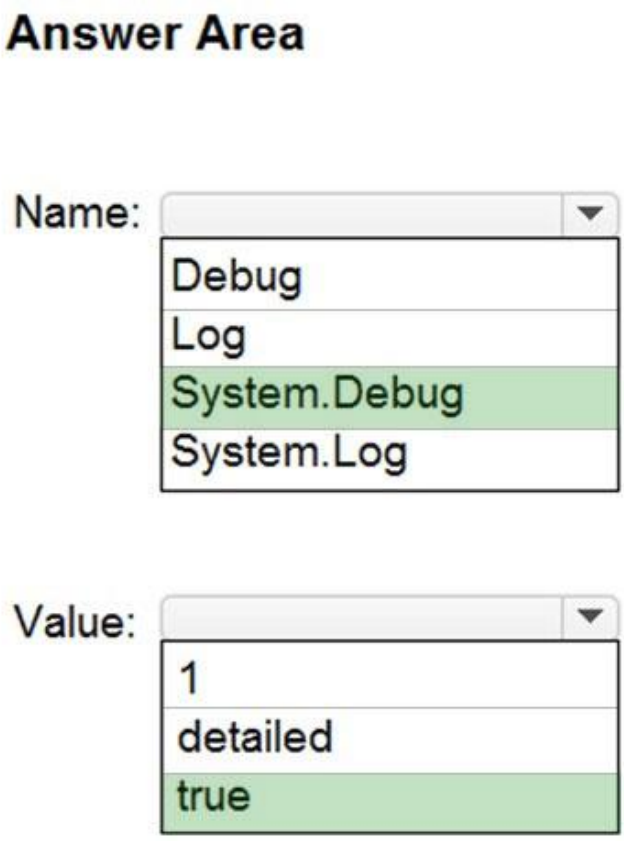
Question #29*Topic 2*

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:



Hide Solution Discussion 8

Correct Answer:



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 #30*Topic 2*

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. **Most Voted**
- C. Configure the Crashlytics pod in the app.
- D. Import the Firebase module to UIApplicationDelegate. **Most Voted**

Hide Solution | Discussion 13

Correct Answer: *D*
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

Community vote distribution

D (75%)
B (25%)

Question #31*Topic 2*

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. **Most Voted**
- D. Create a custom query to show the consumers and producers and add a widget to a dashboard.

Hide Solution | Discussion 1

Correct Answer: *C*

Community vote distribution

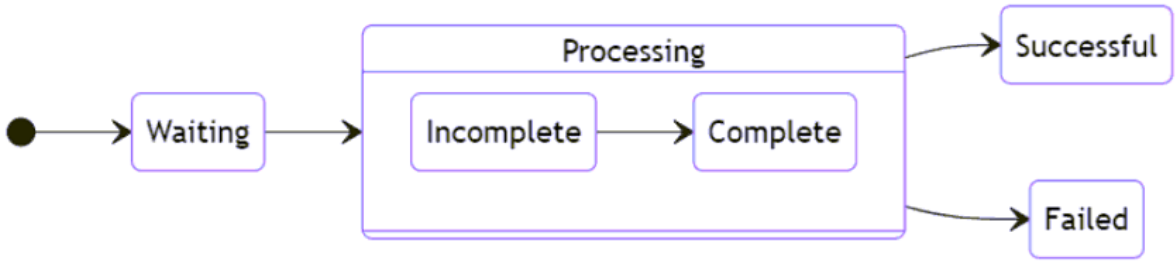
C (100%)

Question #32*Topic 2*

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

Hide Solution Discussion 1

Answer Area

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

Correct Answer:

Question #33*Topic 2*

HOTSPOT
-

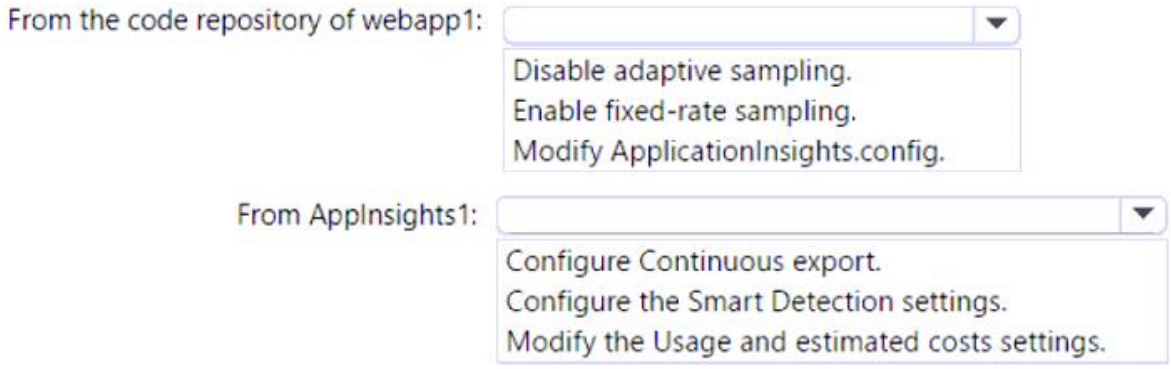
You have an Azure web app named webapp1 that uses the .NET Core runtime stack. You have an Azure Application Insights resource named AppInsights1 that collects telemetry data generated by webapp1.

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.

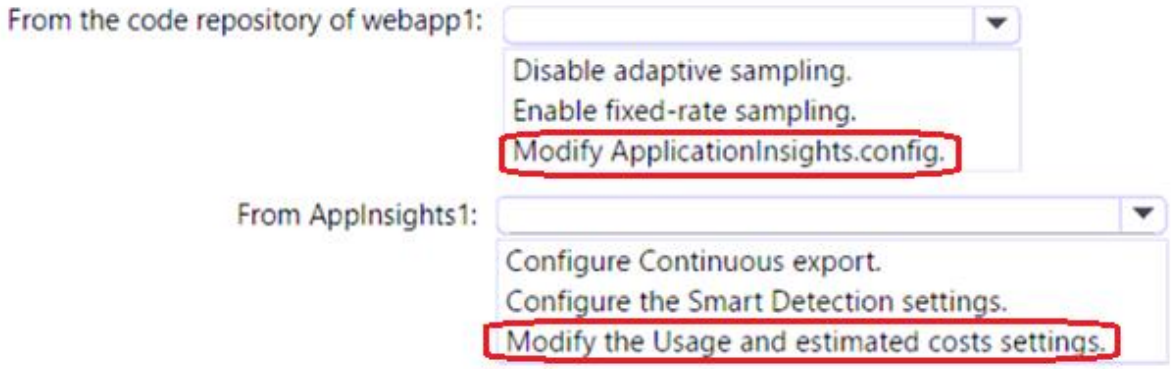
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Hide Solution Discussion 4

Correct Answer:



Question #34*Topic 2*

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. OpenTelemtry **Most Voted**
- E. OpenCensus **Most Voted**

Hide Solution | Discussion 1

Correct Answer: *DE*

Community vote distribution

DE (100%)

Question #35*Topic 2*

You have an Azure web app named webapp1 that uses the .NET Core runtime stack. You have an Azure Application Insights resource named AppInsights1. Webapp1 sends telemetry data to AppInsights1.

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. **Most Voted**
- B. From the code repository of webapp1, modify the Startup.cs file. **Most Voted**
- C. From AppInsights1, modify the Usage and estimated costs settings.
- D. From AppInsights1, configure the Continuous export settings.

Hide Solution | Discussion 12

Correct Answer: *B*

Community vote distribution

B (45%)
A (45%)
9%

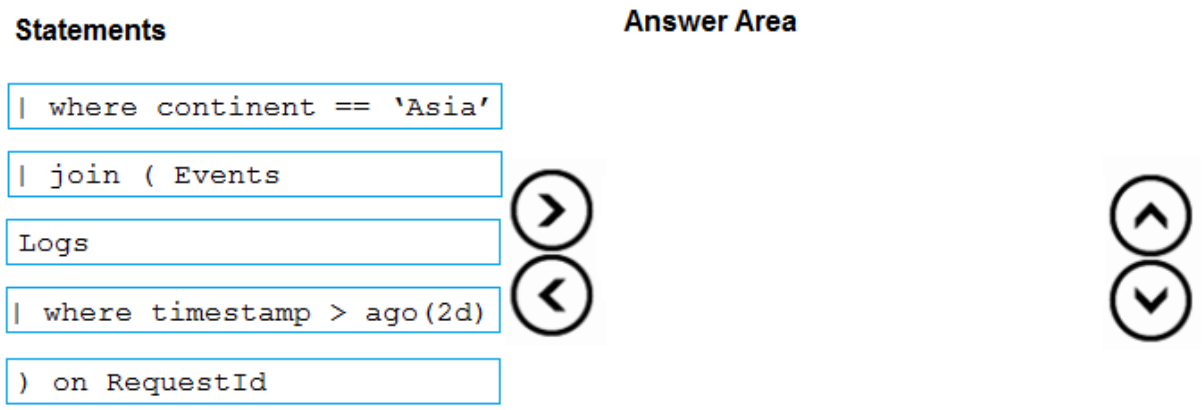
Question #36*Topic 2*

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.

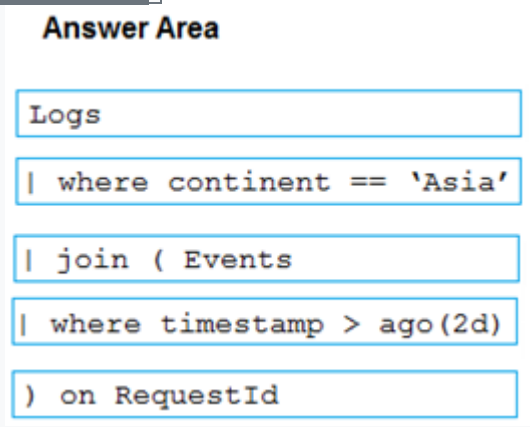
You need to query Workspace1 for all log entries related to Asia that occurred during the last two days.

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.



Hide Solution Discussion 2

Correct Answer:



3 Topic 3 - Question Set 3

Question #1*Topic 3*

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. **Most Voted**
- D. Create and configure an action group. **Most Voted**

Hide Solution Discussion 7

Correct Answer: *CD*
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/
Community vote distribution

CD (100%)

Question #2*Topic 3*

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

Hide Solution | Discussion 5

Correct Answer: *B*
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
Community vote distribution

B (88%)

13%

Question #3*Topic 3*

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. **Most Voted**
- 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.

Hide Solution | Discussion 9

Correct Answer: *B*
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
Community vote distribution

B (100%)

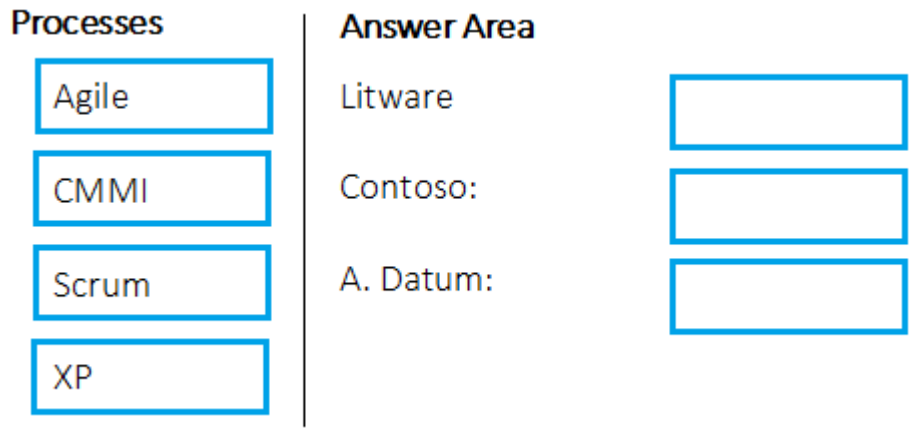
Question #4*Topic 3*

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

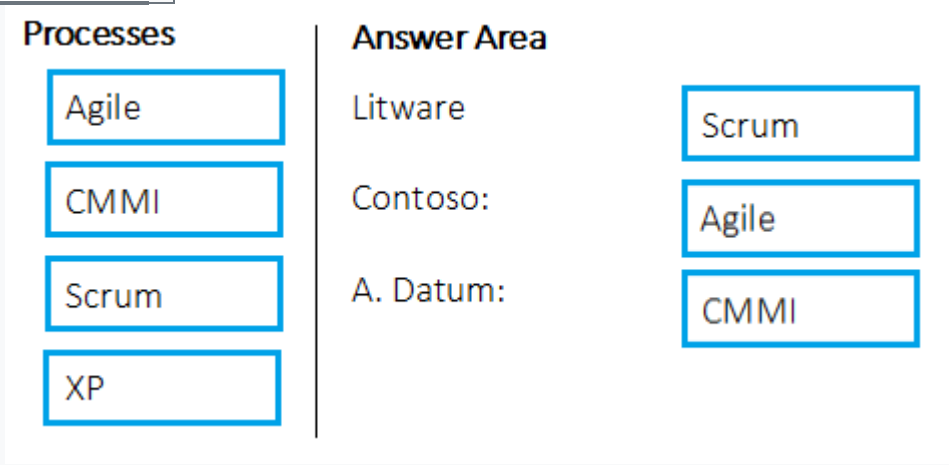
Customer name	Preferred process
Litware, Inc.	Track product backlog items (PBIs) and bugs on the Kanban board. Break the PBIs down into tasks on the task board.
Contoso, Ltd.	Track user stories and bugs on the Kanban board. Track the bugs and tasks on the task board.
A. Datum Corporation	Track requirements,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



Hide Solution Discussion 17



Correct Answer:

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 #5*Topic 3*

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 **Most Voted**
- D. an ApiConnection trigger

Hide Solution | Discussion 46

Correct Answer: *A*
You can use webhooks to route an Azure alert notification to other systems for post-processing or custom actions. You can use a webhook on an alert to route it to services that send SMS messages, to log bugs, to notify a team via chat or messaging services, or for various other actions.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-webhooks

Community vote distribution

C (90%)
7%

Question #6*Topic 3*

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. **Most Voted**
- 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.

Hide Solution | Discussion 43

Correct Answer: *B*
For containerized applications that serve traffic, you might want to verify that your container is ready to handle incoming requests. Azure Container Instances supports readiness probes to include configurations so that your container can't be accessed under certain conditions. The readiness probe behaves like a
Kubernetes readiness probe. For example, a container app might need to load a large data set during startup, and you don't want it to receive requests during this time.
YAML is used to setup a liveness probe.

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

Community vote distribution

A (100%)

Question #7*Topic 3*

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 **Most Voted**

Hide Solution | Discussion 19

Correct Answer: *D*
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

Community vote distribution

D (80%)
C (20%)

Question #8*Topic 3*

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 **Most Voted**
- 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

Hide Solution Discussion 15

Correct Answer: *A*
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
Community vote distribution
A (100%)

Question #9*Topic 3*

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.

Hide Solution Discussion 9

Correct Answer: *See explanation below.*
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 #10*Topic 3*

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) identifies.
☞ 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 **Most Voted**

Hide Solution Discussion 37

Correct Answer: *C*
There are several tools available for running queries in Azure Data Explorer, including Kusto.
Kusto uses a role-based access control (RBAC) model, under which authenticated principals are mapped to roles, and get access according to the roles they're assigned.
Note: Azure Data Explorer is a highly scalable and secure analytics service that enables you to do rich exploration of structured and unstructured data for instant insights. Optimized for ad-hoc queries, Azure Data Explorer enables rich data exploration over raw, structured, and semi-structured data delivering fast time to insight. Query with a modern, intuitive query language that offers fast, ad-hoc, and advanced query capabilities over high-rate data volumes and varieties
Reference:
https://docs.microsoft.com/en-us/azure/data-explorer/tools-integrations-overview
Community vote distribution
D (100%)

Question #11*Topic 3*

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 **Most Voted**
- C. Xamarin.UITest
- D. Microsoft.CodeAnalysis

Hide Solution Discussion 22

Correct Answer: *B*
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
Community vote distribution
B (89%)
11%

Question #12*Topic 3*

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. **Most Voted**
- D. Add the <MaxTelemetryItemsPerSecond>5</MaxTelemetryItemsPerSecond> parameter to the ApplicationInsights.config file.
- E. From the code of the application, disable adaptive sampling. **Most Voted**

Hide Solution | Discussion 46

Correct Answer: *BD*

Sampling is a feature in Azure Application Insights. It is the recommended way to reduce telemetry traffic, data costs, and storage costs, while preserving a statistically correct analysis of application data.
The Application Insights SDK for ASP.NET Core supports both fixed-rate and adaptive sampling. Adaptive sampling is enabled by default.
D: For adaptive sampling: The volume is adjusted automatically to keep within a specified maximum rate of traffic, and is controlled via the setting MaxTelemetryItemsPerSecond. If the application produces a low amount of telemetry, such as when debugging or due to low usage, items won't be dropped by the sampling processor as long as volume is below MaxTelemetryItemsPerSecond.
Note: In ApplicationInsights.config, you can adjust several parameters in the AdaptiveSamplingTelemetryProcessor node. The figures shown are the default values:
<MaxTelemetryItemsPerSecond>5</MaxTelemetryItemsPerSecond>
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/sampling

Community vote distribution

CE (62%)
CD (15%)
BC (15%)
8%

Question #13*Topic 3*

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 **Most Voted**

Hide Solution Discussion 14

Correct Answer: *D*

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-extension

Community vote distribution

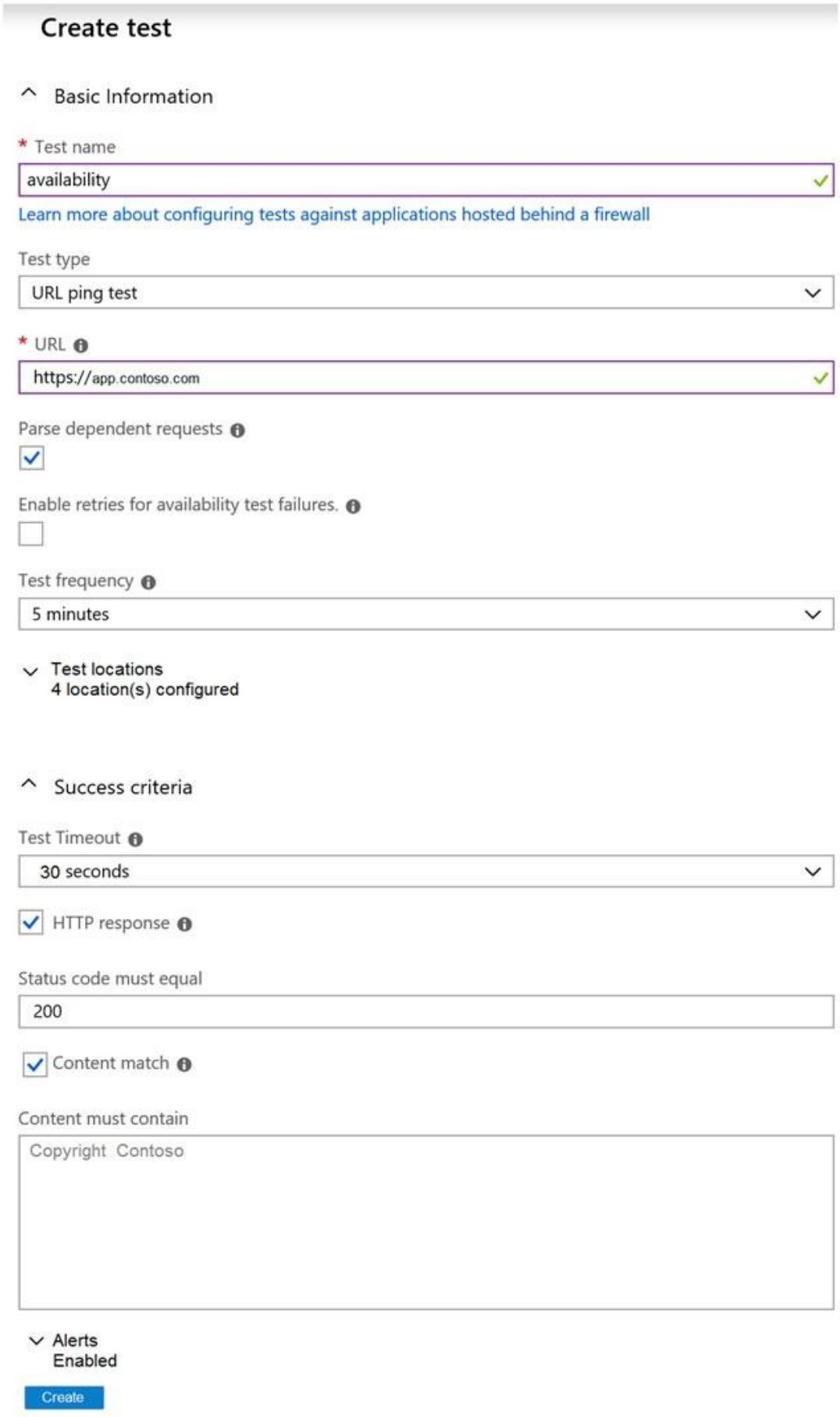
D (100%)

Question #14*Topic 3*

HOTSPOT -

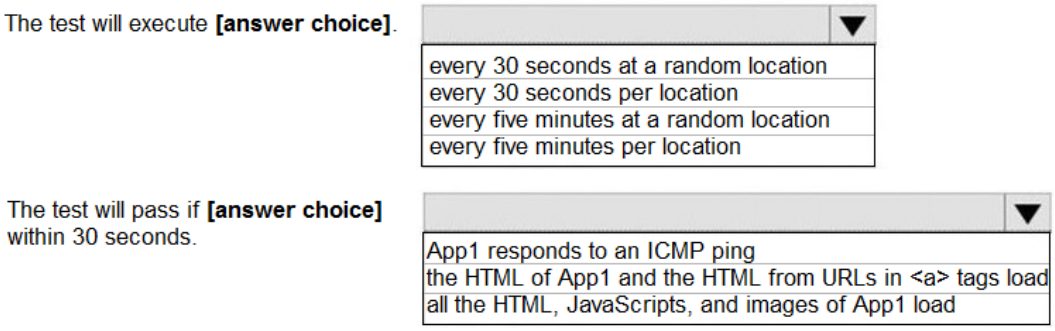
You have an application named App1 that has a custom domain of app.contoso.com.

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
Copyright Contoso
Alerts
Enabled
Create

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.
Hot Area:

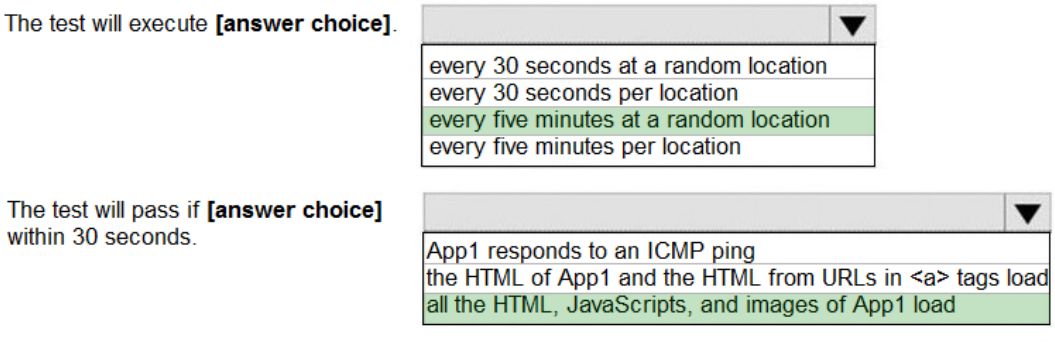
Answer Area



Hide Solution Discussion 24

Correct Answer:

Answer Area



Box 1: every five minutes at a random location
Test frequency: Sets how often the test is run from each test location. With a default frequency of five minutes and five test locations, your site is tested on average every minute.
Box 2:
Parse dependent requests: Test requests images, scripts, style files, and other files that are part of the web page under test. The recorded response time includes the time taken to get these files. The test fails if any of these resources cannot be successfully downloaded within the timeout for the whole test.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability

Question #15*Topic 3*

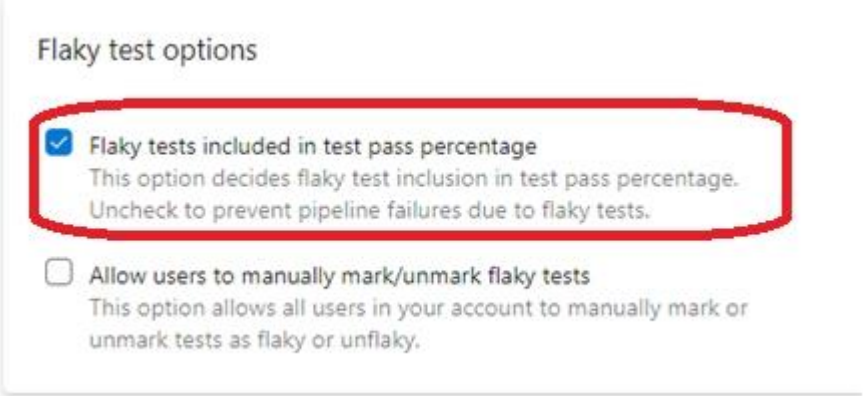
You have a build pipeline in Azure Pipelines that occasionally fails.
You discover that a test measuring the response time of an API endpoint causes the failures.
You need to prevent the build pipeline from failing due to the test.

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. **Most Voted**
- C. Enable Test Impact Analysis (TIA).
- D. Manually mark the test as flaky. **Most Voted**
- E. Enable test slicing.

Hide Solution | Discussion 11

Correct Answer: *BD*
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
Community vote distribution
BD (100%)

Question #16*Topic 3*

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

Hide Solution | Discussion 11

Correct Answer: *C*
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
Community vote distribution
C (100%)

Question #17*Topic 3*

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

Reveal Solution Discussion 9

Question #18*Topic 3*

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 **Most Voted**
- D. Azure Active Directory (Azure AD)
- E. The Windows Server 2019 container images hosted in the Azure Container Registry. **Most Voted**

Hide Solution | Discussion 45

Correct Answer: *BC*
B: Azure Security Center includes Azure-native, advanced threat protection for Azure Key Vault, providing an additional layer of security intelligence.
C: When Security Center discovers a connected VM without a vulnerability assessment solution deployed, it provides the security recommendation "A vulnerability assessment solution should be enabled on your virtual machines".
Ubuntu supported versions: 12.04 LTS, 14.04 LTS, 15.x, 16.04 LTS, 18.04 LTS
Reference:
https://docs.microsoft.com/en-us/azure/security-center/deploy-vulnerability-assessment-vm
Community vote distribution

CE (82%)
BC (18%)

Question #19*Topic 3*

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.

Hide Solution | Discussion 15

Correct Answer: *B*
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/
Community vote distribution

B (100%)

Question #20*Topic 3*

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

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

Hide Solution Discussion 6

Correct Answer: *B*
Instead implement Continuous Assurance for the project.
Reference:
https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html
Community vote distribution
B (100%)

Question #21*Topic 3*

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

Reveal Solution Discussion 9

Question #22*Topic 3*

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

Hide Solution Discussion 9

Correct Answer: *A*

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‚Ä¶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

Community vote distribution

A (100%)

Question #23*Topic 3*

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

Hide Solution Discussion 6

Correct Answer: *C*
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
Community vote distribution
C (100%)

Question #24*Topic 3*
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 **Most Voted**
- D. an Azure Load Balancer health probe

Hide Solution | Discussion 11

Correct Answer: *C*
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
Community vote distribution
C (100%)

Question #25*Topic 3*

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 **Most Voted**
- C. the Azure Network Watcher Agent for Windows
- D. the Dependency agent **Most Voted**

Hide Solution | Discussion 10

Correct Answer: *BD*
The following table provide a quick comparison of the Azure Monitor agents for Windows.

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

Community vote distribution

BD (100%)

Question #26*Topic 3*

DRAG DROP -

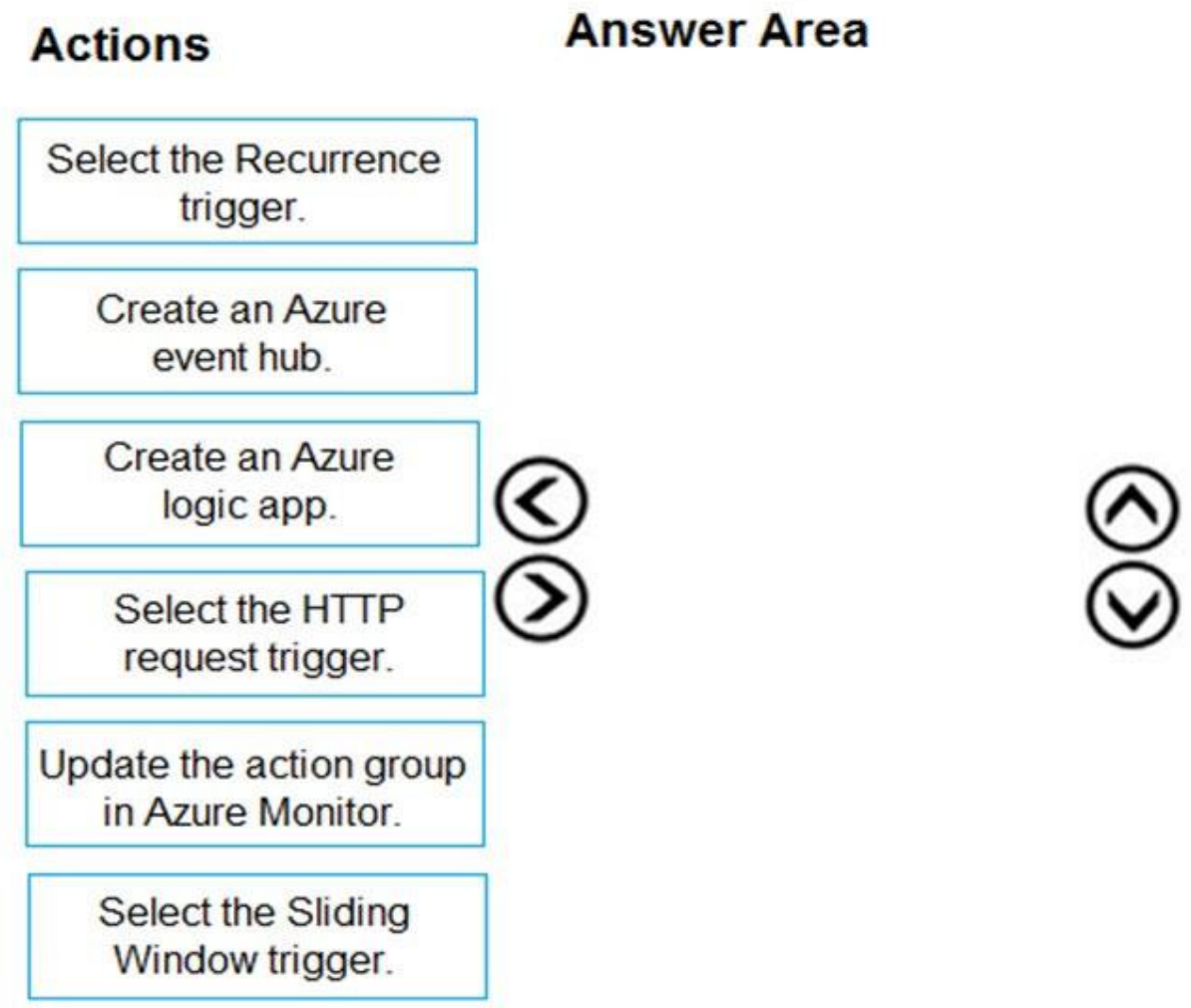
You use Azure Pipelines to automate Continuous Integration/Continuous Deployment (CI/CD) for an Azure web app named WebApp1.

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.

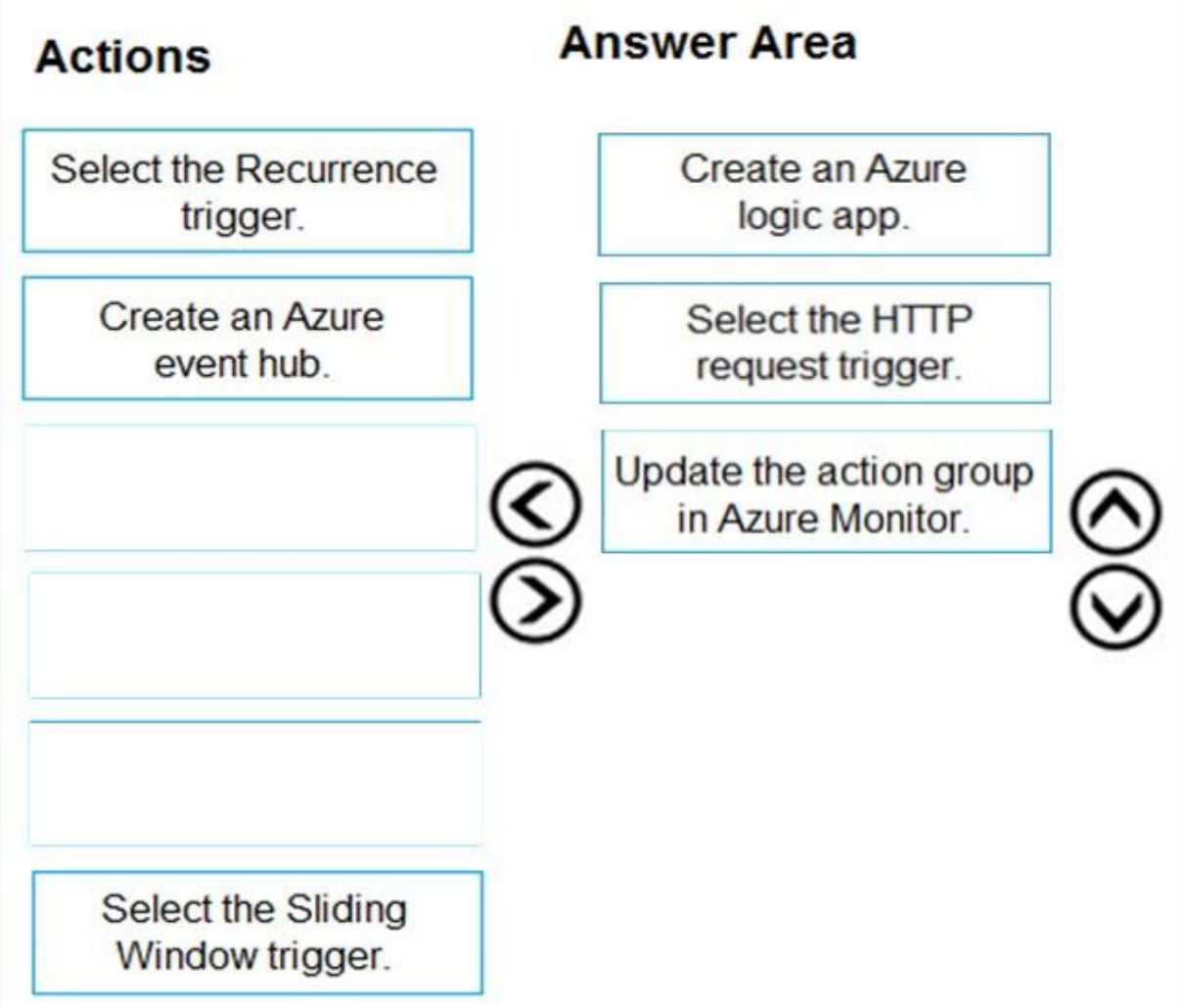
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Hide Solution Discussion 6

Correct Answer:



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 #27*Topic 3*

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

Hide Solution | Discussion 6

Correct Answer: *B*

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

Community vote distribution

B (100%)

Question #28*Topic 3*

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

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

You 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 **Most Voted**

Hide Solution | Discussion 4

Correct Answer: *B*

Community vote distribution

B (100%)

Question #29*Topic 3*

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

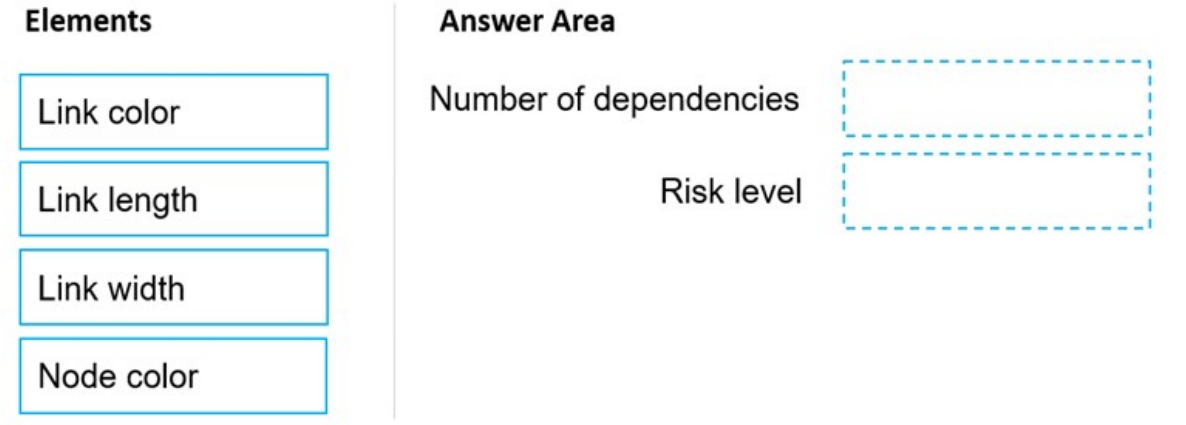
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 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 **Most Voted**
- B. No

Hide Solution | Discussion 6

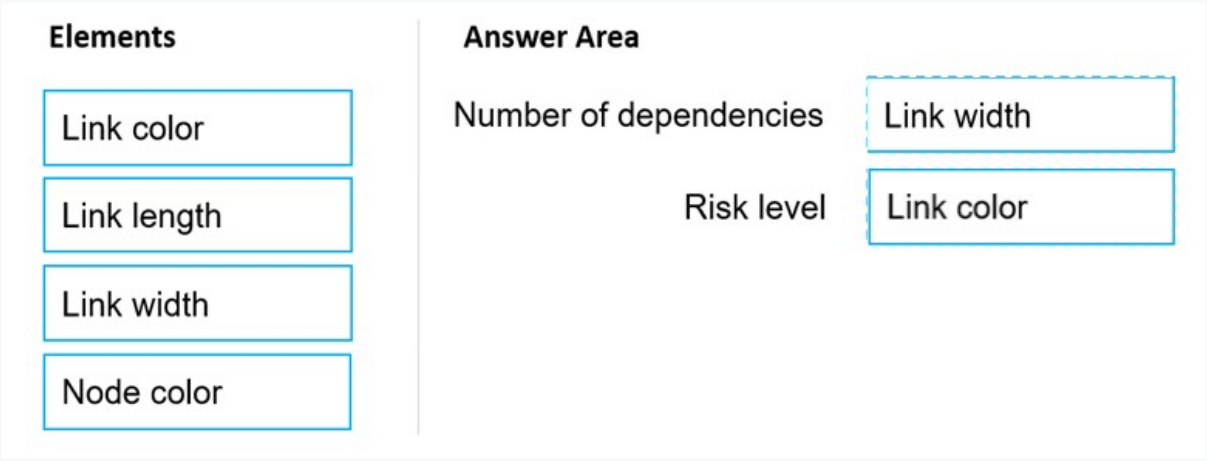
Correct Answer: *A*
An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor, Service Health and Azure Advisor alerts use action groups to notify users that an alert has been triggered.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups
Community vote distribution
A (100%)

Question #30*Topic 3*
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:



Hide Solution | Discussion 3

Correct Answer:



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

4 Topic 4 - Question Set 4

Question #1*Topic 4*

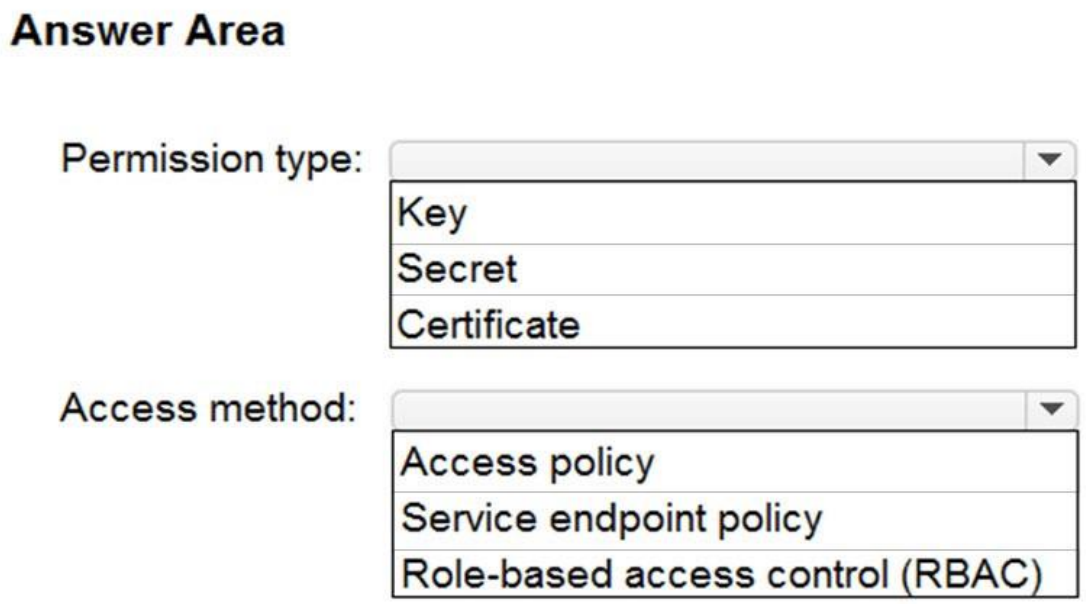
HOTSPOT -
You have an Azure subscription that contains the resources shown in the following table.

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

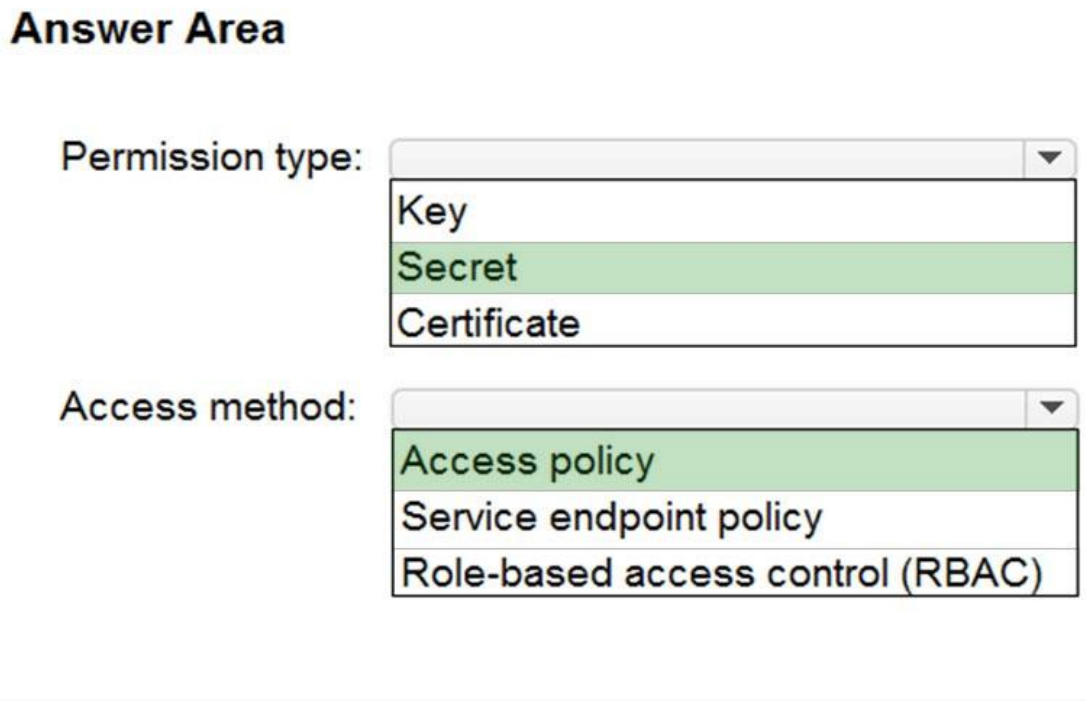
Server login will be stored -
in KV1.
You need to configure DF1 to retrieve the password when the data factory connects to SQL1. The solution must use the principle of least privilege.
How should you configure DF1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Hide Solution Discussion 6

Correct Answer:



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 #2*Topic 4*

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 **Most Voted**

Hide Solution | Discussion 8

Correct Answer: *D*
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

Community vote distribution
D (100%)

Question #3*Topic 4*

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) **Most Voted**
- B. SSH key
- C. Alternate credentials
- D. certificate

Hide Solution | Discussion 16

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

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

Community vote distribution

A (100%)

Question #4*Topic 4*

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 **Most Voted**
- 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

Hide Solution | Discussion 12

Correct Answer: *B*
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

Community vote distribution

B (100%)

Question #5*Topic 4*

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 **Most Voted**
- B. Alternate credentials in Azure DevOps
- C. user accounts in Azure Active Directory (Azure AD)
- D. managed identities in Azure Active Directory (Azure AD)

Hide Solution | Discussion 10

Correct Answer: *A*
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
Community vote distribution

A (100%)

Question #6*Topic 4*

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 **Most Voted**

Hide Solution | Discussion 14

Correct Answer: *D*
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
Community vote distribution

D (100%)

Question #7*Topic 4*

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 Manger templates. **Most Voted**

Hide Solution | Discussion 59

Correct Answer: *B*

Azure Key Vault provides a way to securely store credentials and other keys and secrets.
The Set-AzureKeyVaultSecret cmdlet creates or updates a secret in a key vault in Azure Key Vault.
Reference:
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecret

Community vote distribution

D (93%)
7%

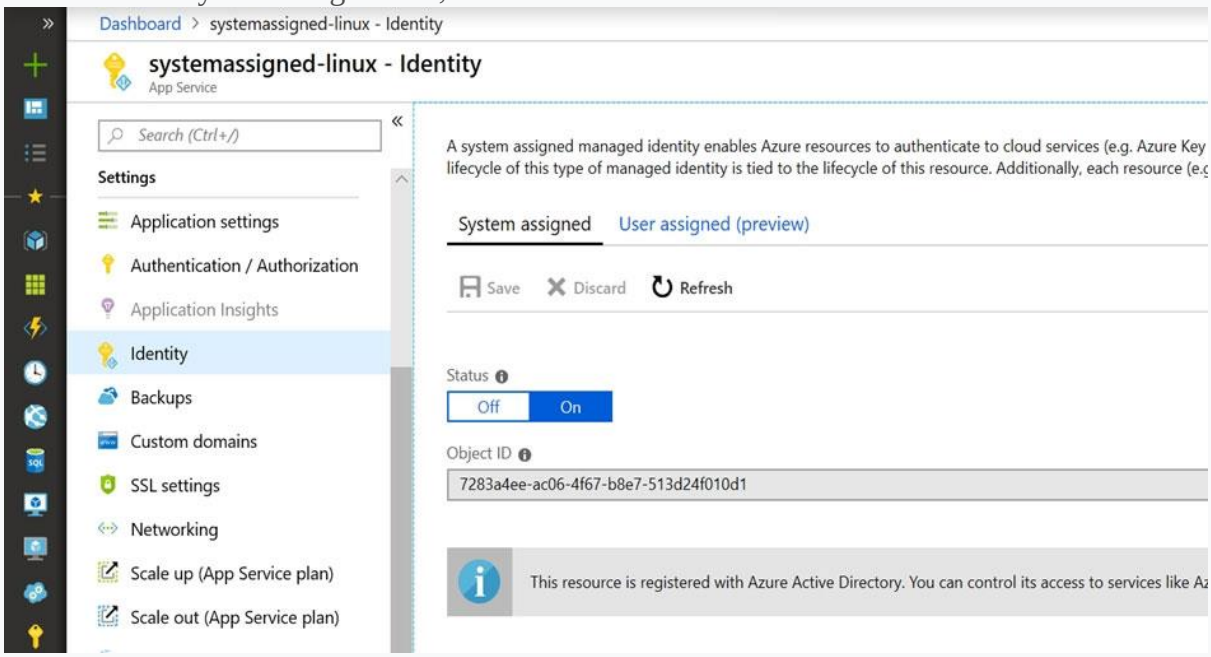
Question #8*Topic 4*

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.

Hide Solution | Discussion 2

Correct Answer: *See explanation below.*

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.



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

Question #9*Topic 4*

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?

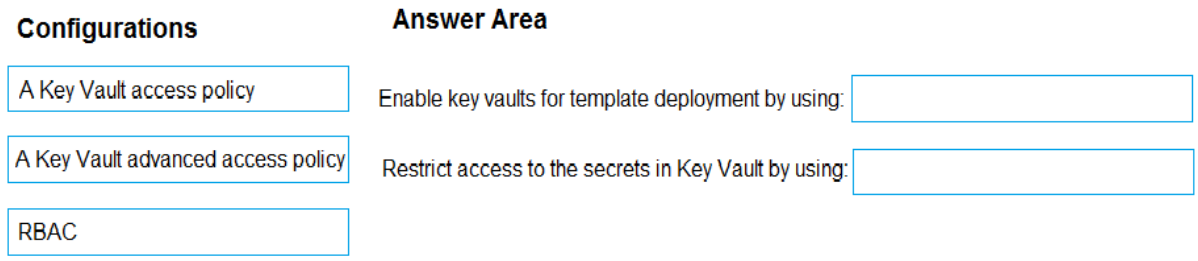
- A. List only
- B. Get only **Most Voted**
- C. Get and List

Hide Solution | Discussion 34

Correct Answer: *B*
Application data plane permissions:
☞ Keys: sign
☞ Secrets: get
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault
Community vote distribution
B (91%)
9%

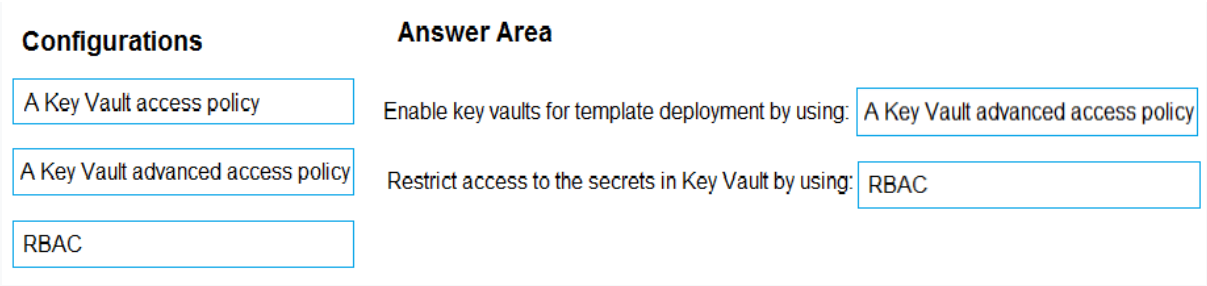
Question #10*Topic 4*

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:

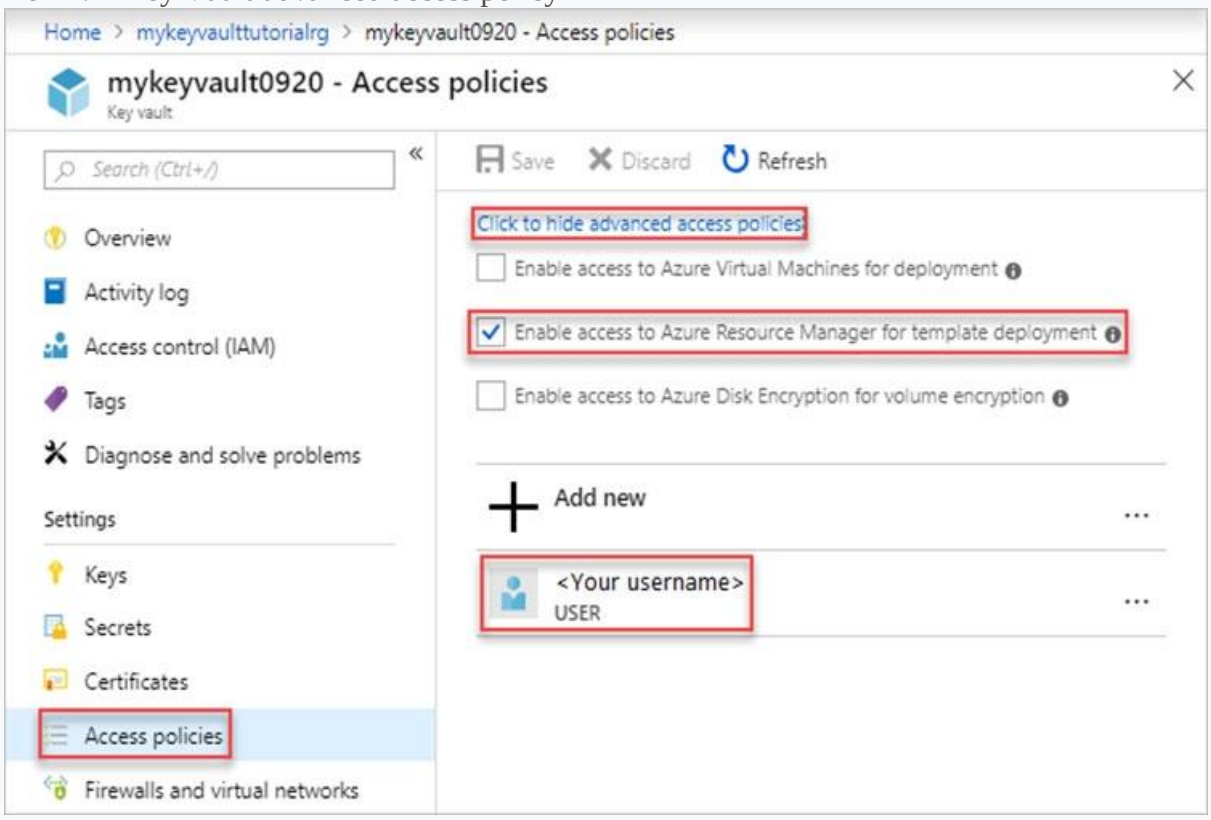


Hide Solution | Discussion 40

Correct Answer:



Box 1: A key Vault advanced access policy



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.

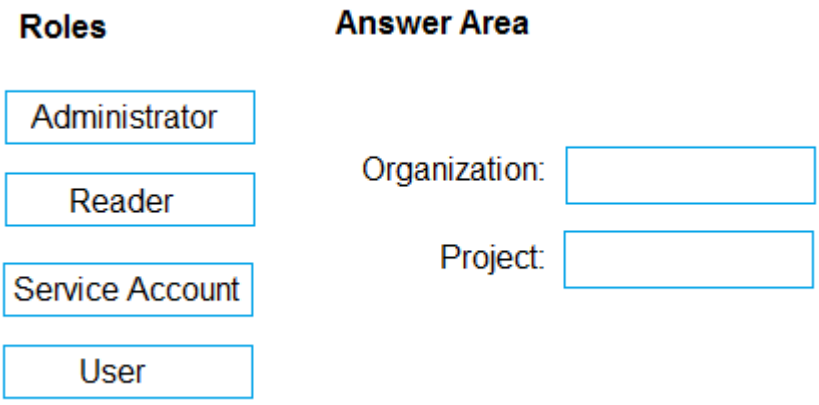
Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-tutorial-use-key-vault

Question #11*Topic 4*

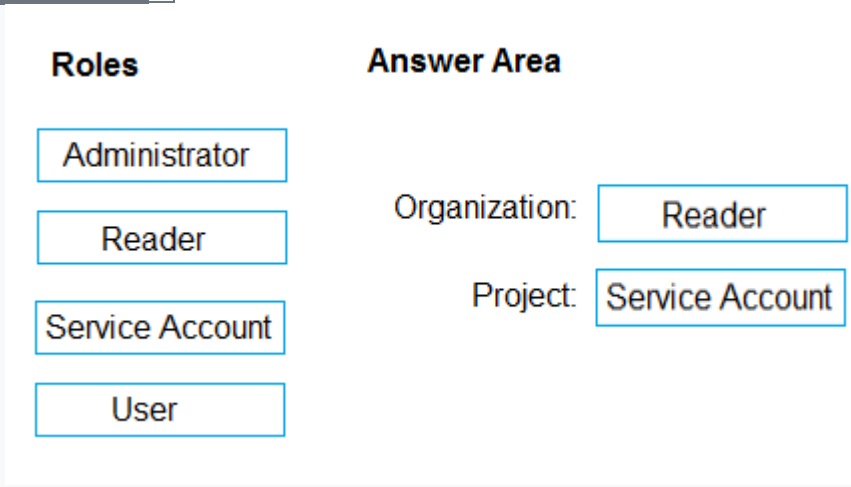
DRAG DROP -
You need to configure access to Azure DevOps agent pools to meet the following requirements:

- 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:



Hide Solution Discussion 46



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

Box 2: Service account -
Members of the Service account role can use the organization agent pool to create a project agent pool in a project. If you follow the guidelines above for creating new project agent pools, you typically do not have to add any members here.
Incorrect Answers:
In addition to all the permissions given the Reader and the Service Account role, members of the administrator role can register or unregister agents from the organization agent pool. They can also refer to the organization agent pool when creating a project agent pool in a project.

Finally, they can also manage membership for all roles of the organization agent pool. The user that created the organization agent pool is automatically added to the Administrator role for that pool.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues

Question #12*Topic 4*

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.

Hide Solution | Discussion 14

Correct Answer: *D*
In some cases, you need to bypass policy requirements so you can push changes to the branch directly or complete a pull request even if branch policies are not satisfied. For these situations, grant the desired permission from the previous list to a user or group. You can scope this permission to an entire project, a repo, or a single branch. Manage this permission along the with other Git permissions.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies
Community vote distribution
D (100%)

Question #13*Topic 4*

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

Hide Solution | Discussion 12

Correct Answer: *A*
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

Community vote distribution

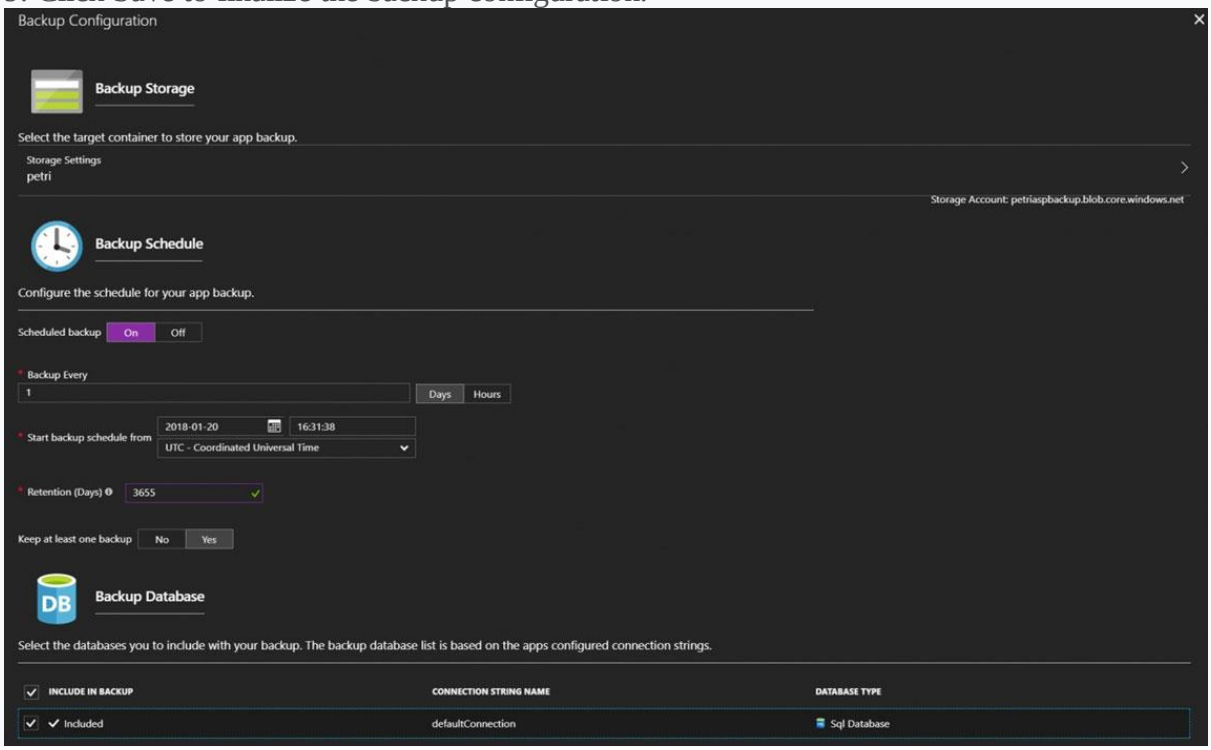
A (100%)

Question #14*Topic 4*

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.

Hide Solution | Discussion 6

Correct Answer: *See explanation below.*
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.



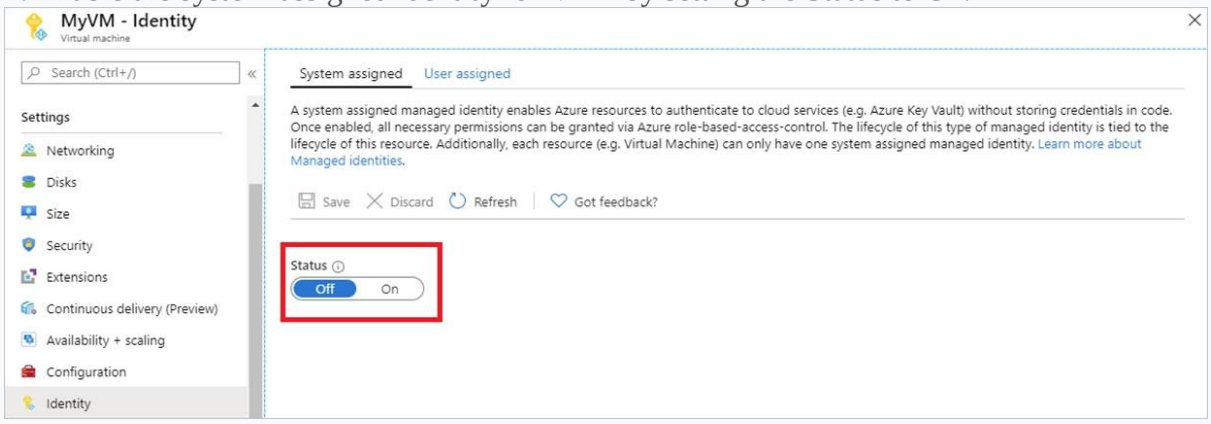
Reference:
https://petri.com/backing-azure-app-service

Question #15*Topic 4*

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.

Hide Solution Discussion 1

Correct Answer: *See explanation below.*
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.

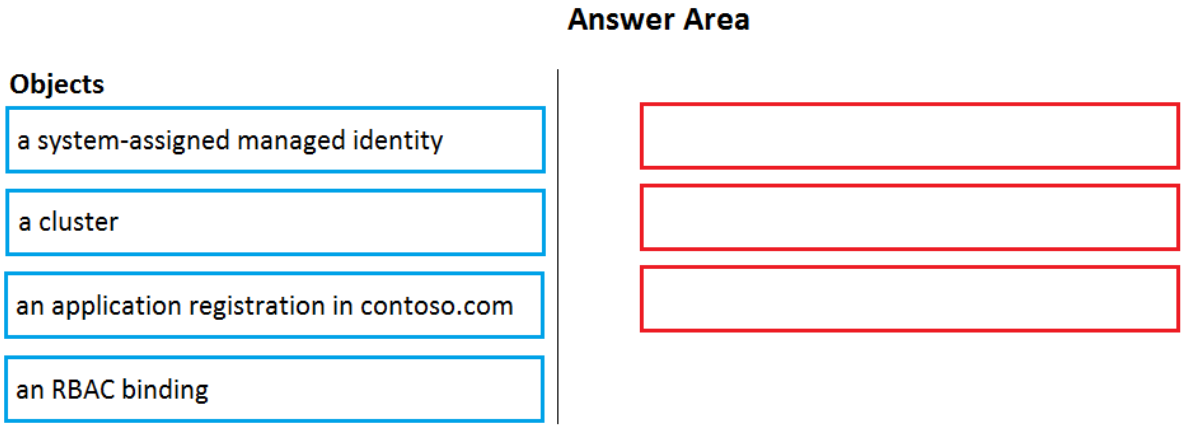


Note: Enabling a system-assigned managed identity is a one-click experience. You can either enable it during the creation of a VM or in the properties of an existing VM.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad

Question #16*Topic 4*

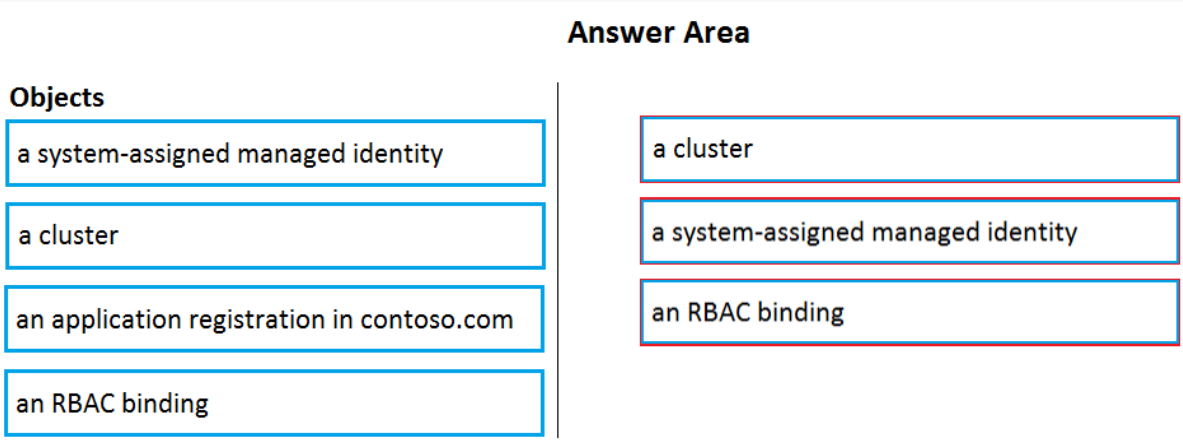
DRAG DROP -
Your company has an Azure subscription named Subscription1. Subscription1 is associated to an Azure Active Directory tenant named contoso.com.
You need to provision an Azure Kubernetes Services (AKS) cluster in Subscription1 and set the permissions for the cluster by using RBAC roles that 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:

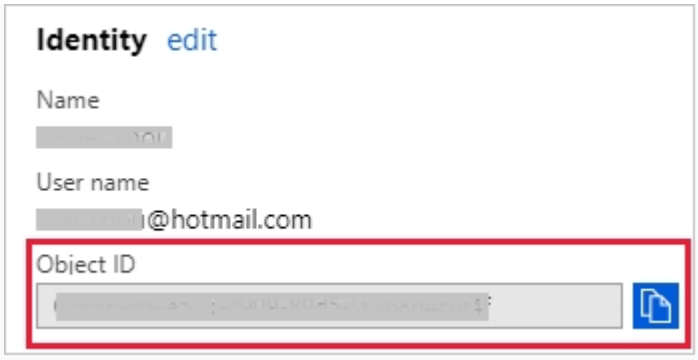


Hide Solution Discussion 17

Correct Answer:



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



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

Question #17*Topic 4*

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

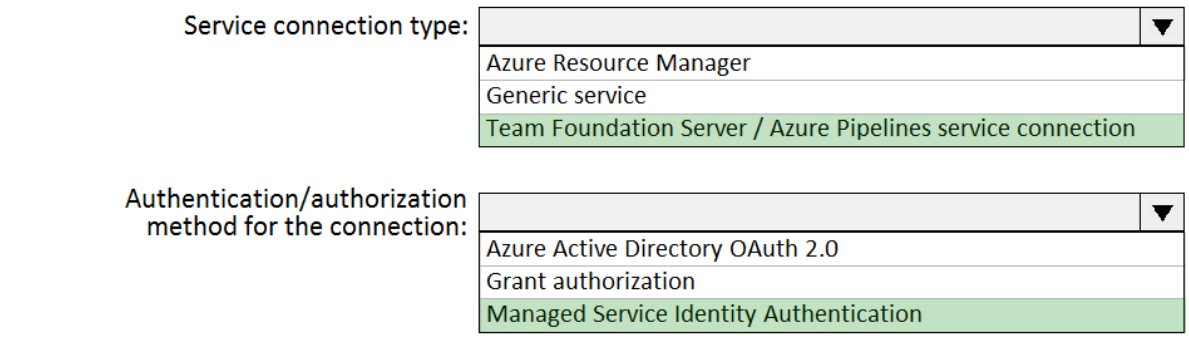
Service connection type:
- Azure Resource Manager
- Generic service
- Team Foundation Server / Azure Pipelines service connection

Authentication/authorization method for the connection:
- Azure Active Directory OAuth 2.0
- Grant authorization
- Managed Service Identity Authentication

Hide Solution | Discussion 19

Correct Answer:

Answer Area



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 #18*Topic 4*

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. **Most Voted**
- C. Configure a Key Vault access policy. **Most Voted**
- D. Deploy an Azure Desired State Configuration (DSC) extension.
- E. Deploy a virtual machine that uses a system-assigned managed identity. **Most Voted**

Hide Solution | Discussion 23

Correct Answer: *BCE*
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

Community vote distribution

BCE (77%)
ABE (15%)
8%

Question #19*Topic 4*

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

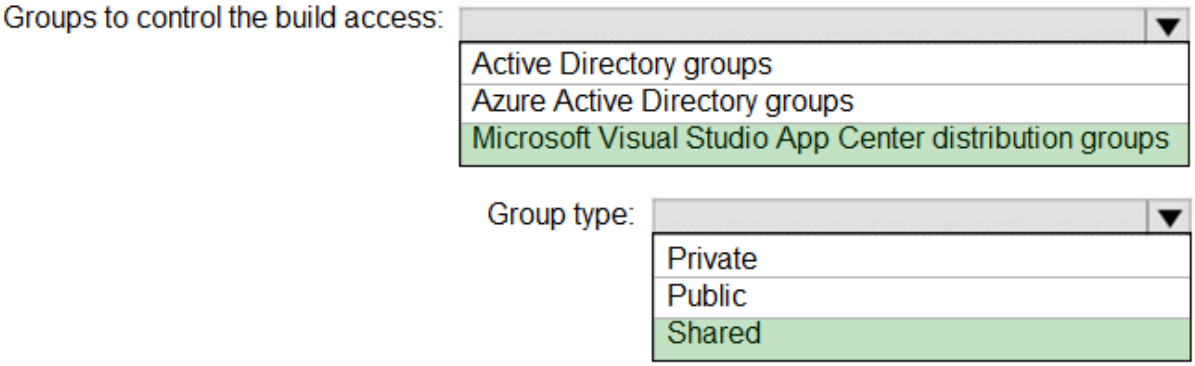
Groups to control the build access:
- Active Directory groups
- Azure Active Directory groups
- Microsoft Visual Studio App Center distribution groups

Group type:
- Private
- Public
- Shared

Hide Solution | Discussion 9

Correct Answer:

Answer Area



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

Question #20*Topic 4*

You have an Azure DevOps organization named Contoso that contains a project named Project1.
You provision an Azure key vault named Keyvault1.
You need to reference Keyvault1 secrets in a build pipeline of Project1.
What should you do first?

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

Hide Solution | Discussion 46

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

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

C (100%)

Question #21*Topic 4*

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.

Hide Solution Discussion 14

Correct Answer: *D*
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
Community vote distribution

D (100%)

Question #22*Topic 4*

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 **Most Voted**
- 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

Hide Solution | Discussion 30

Correct Answer: *B*
Denies non HTTPS traffic.
Community vote distribution
B (91%)
9%

Question #23*Topic 4*

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. **Most Voted**
- B. Add a secure file to Project1.
- C. Modify the security settings of the pipelines.
- D. Configure the security policy of Contoso.

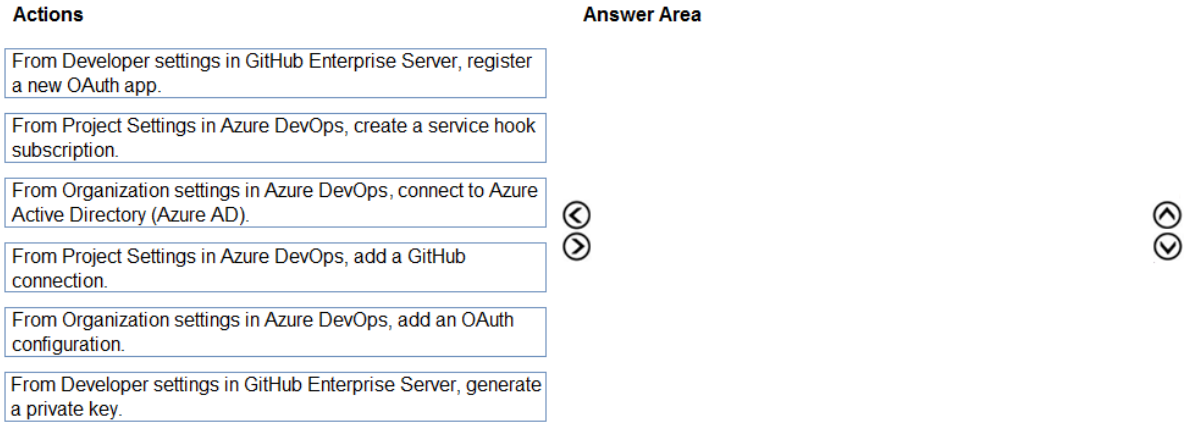
Hide Solution | Discussion 16

Correct Answer: *A*
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
Community vote distribution
A (100%)

Question #24*Topic 4*

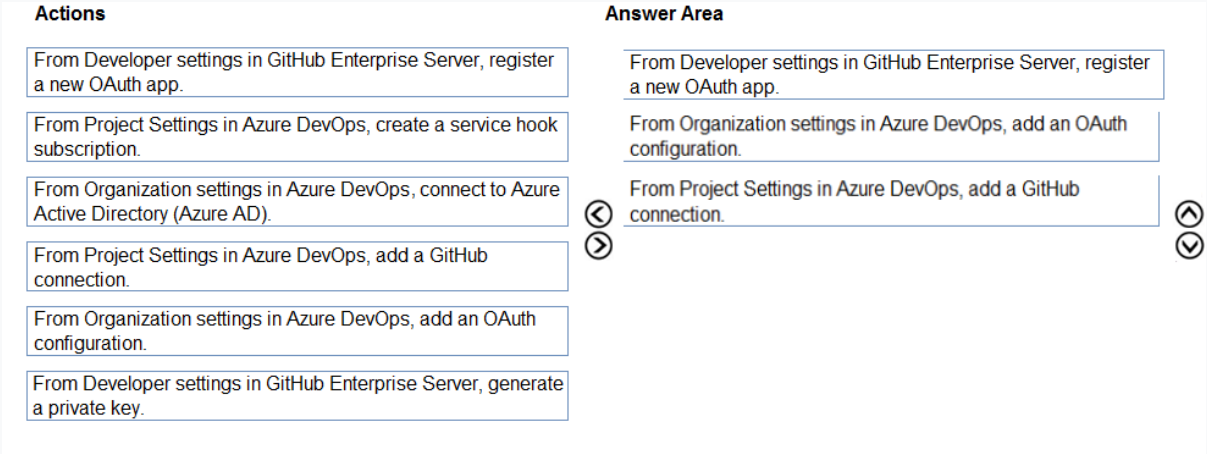
DRAG DROP -
You use GitHub Enterprise Server as a source code repository.
You create an Azure DevOps organization named Contoso.
In the Contoso organization, you create a project named Project1.
You need to link GitHub commits, pull requests, and issues to the work items of Project1.
The solution must 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:



Hide Solution Discussion 8

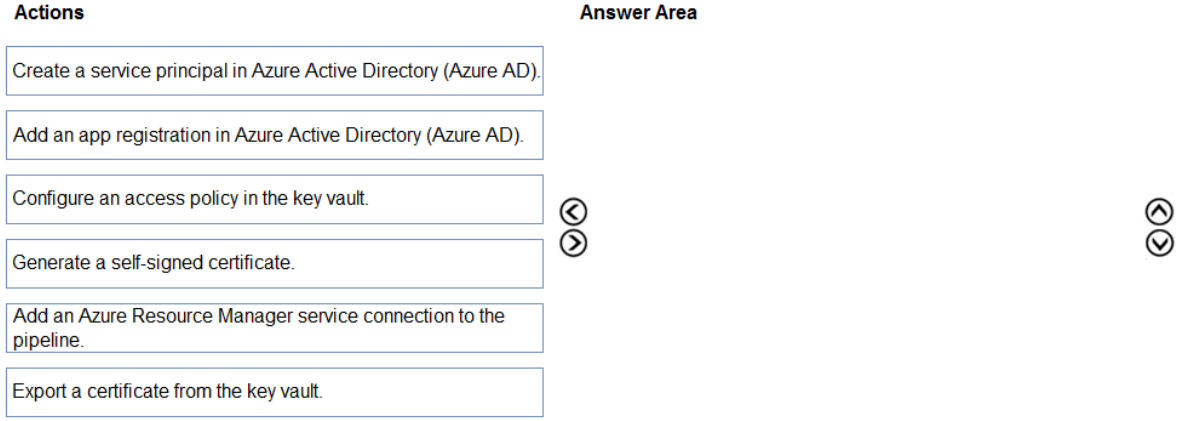
Correct Answer:



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

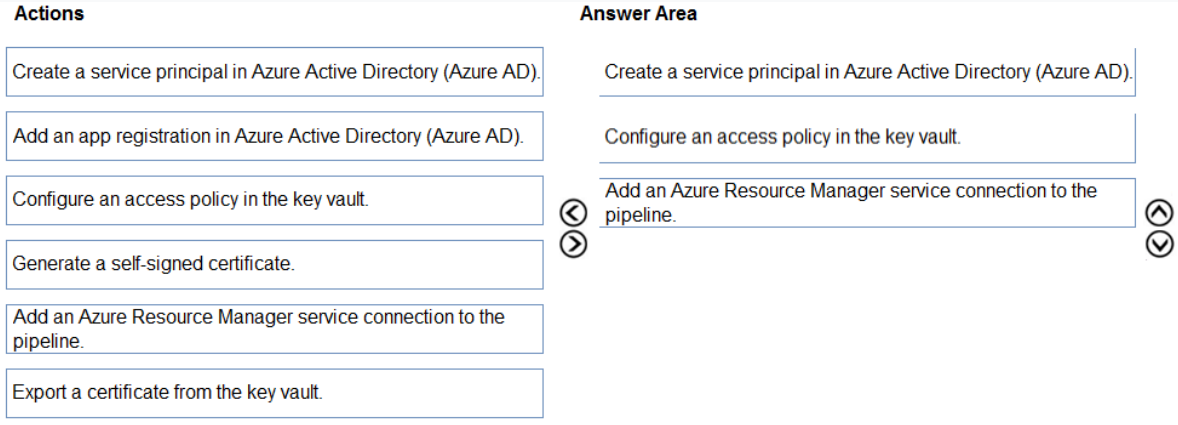
Question #25*Topic 4*

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:

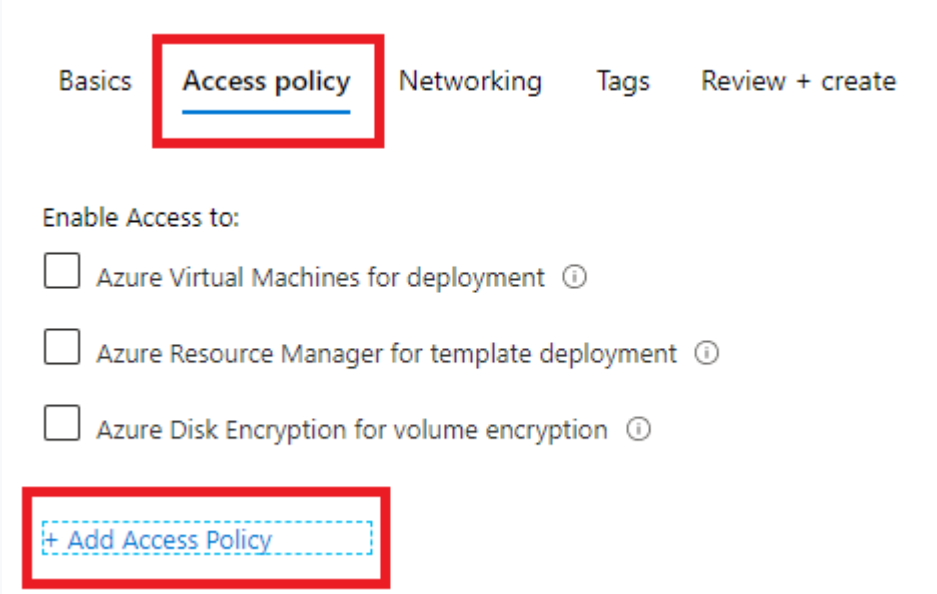


Hide Solution Discussion 34

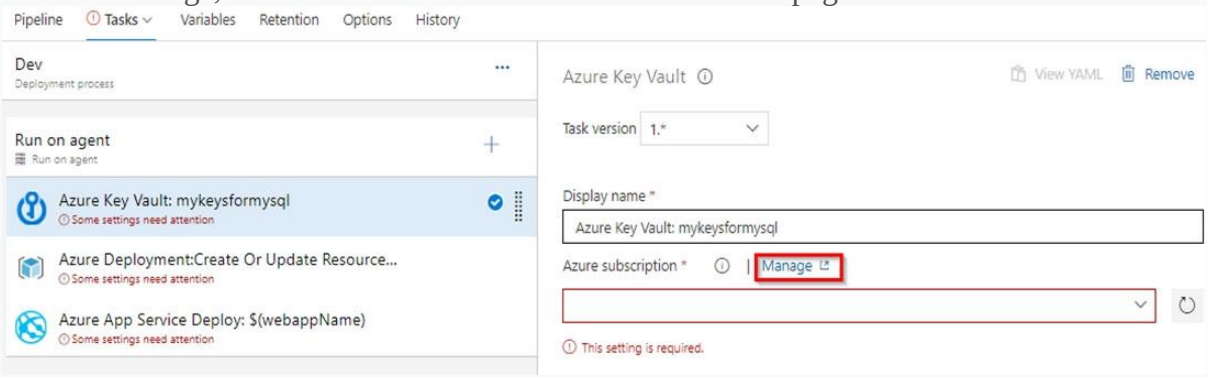
Correct Answer:



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.



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.



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/

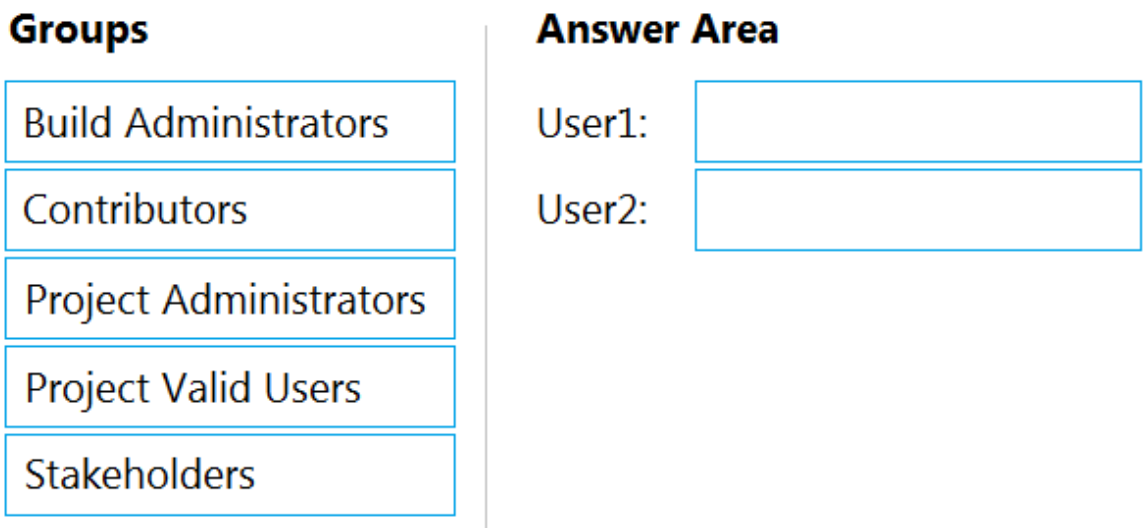
Question #26*Topic 4*

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.

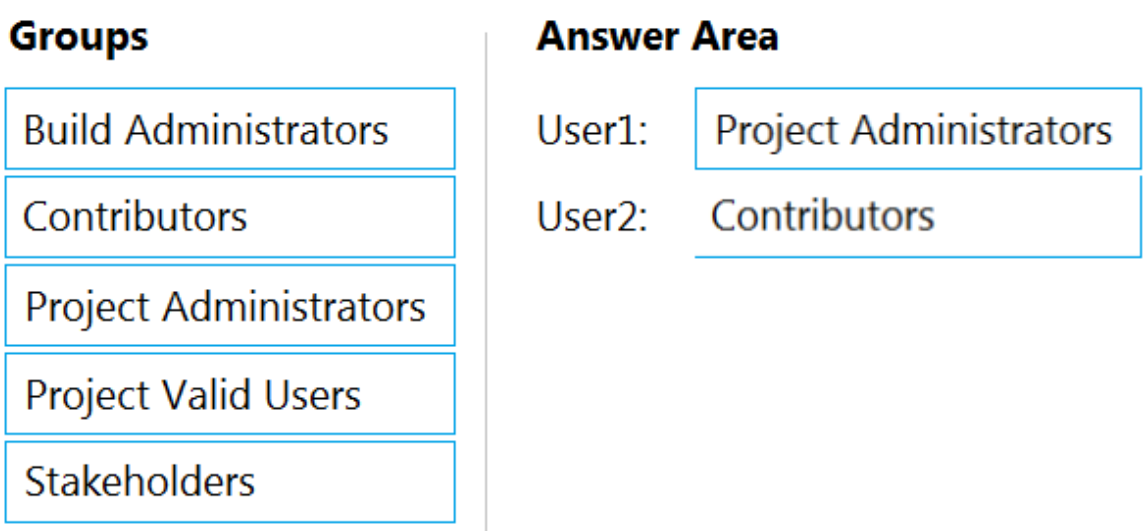
To which group should you add each user? To answer, drag the appropriate groups to the correct users. Each group may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.
Select and Place:



Hide Solution Discussion 16

Correct Answer:



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 #27 *Topic 4*

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. **Most Voted**
- 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. **Most Voted**

Hide Solution | Discussion 24

Correct Answer: *AC*
A: To resolve NPM dependencies, you should first run "npm install" command on the relevant folders before executing the plugin.
C: All npm packages contain a file, usually in the project root, called package.json ‚€" this file holds various metadata relevant to the project. This file is used to give information to npm that allows it to identify the project as well as handle the project's dependencies. It can also contain other metadata such as a project description, the version of the project in a particular distribution, license information, even configuration data ‚€" all of which can be vital to both npm and to the end users of the package.
Reference:
https://whitesource.atlassian.net/wiki/spaces/WD/pages/34209870/NPM+Plugin
https://nodejs.org/en/knowledge/getting-started/npm/what-is-the-file-package-json
Community vote distribution

AD (76%)
12%
12%

Question #28*Topic 4*

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

Hide Solution | Discussion 19

Correct Answer: *A*
WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.
Reference:
https://azuredevopslabs.com/labs/vstsextend/whitesource/
Community vote distribution

B (73%)
A (27%)

Question #29*Topic 4*

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

Hide Solution Discussion 10

Correct Answer: *B*
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/
Community vote distribution

B (100%)

Question #30*Topic 4*

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You 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 **Most Voted**
- B. No

Hide Solution Discussion 14

Correct Answer: *B*
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/
Community vote distribution
A (77%)
B (23%)

Question #31*Topic 4*

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

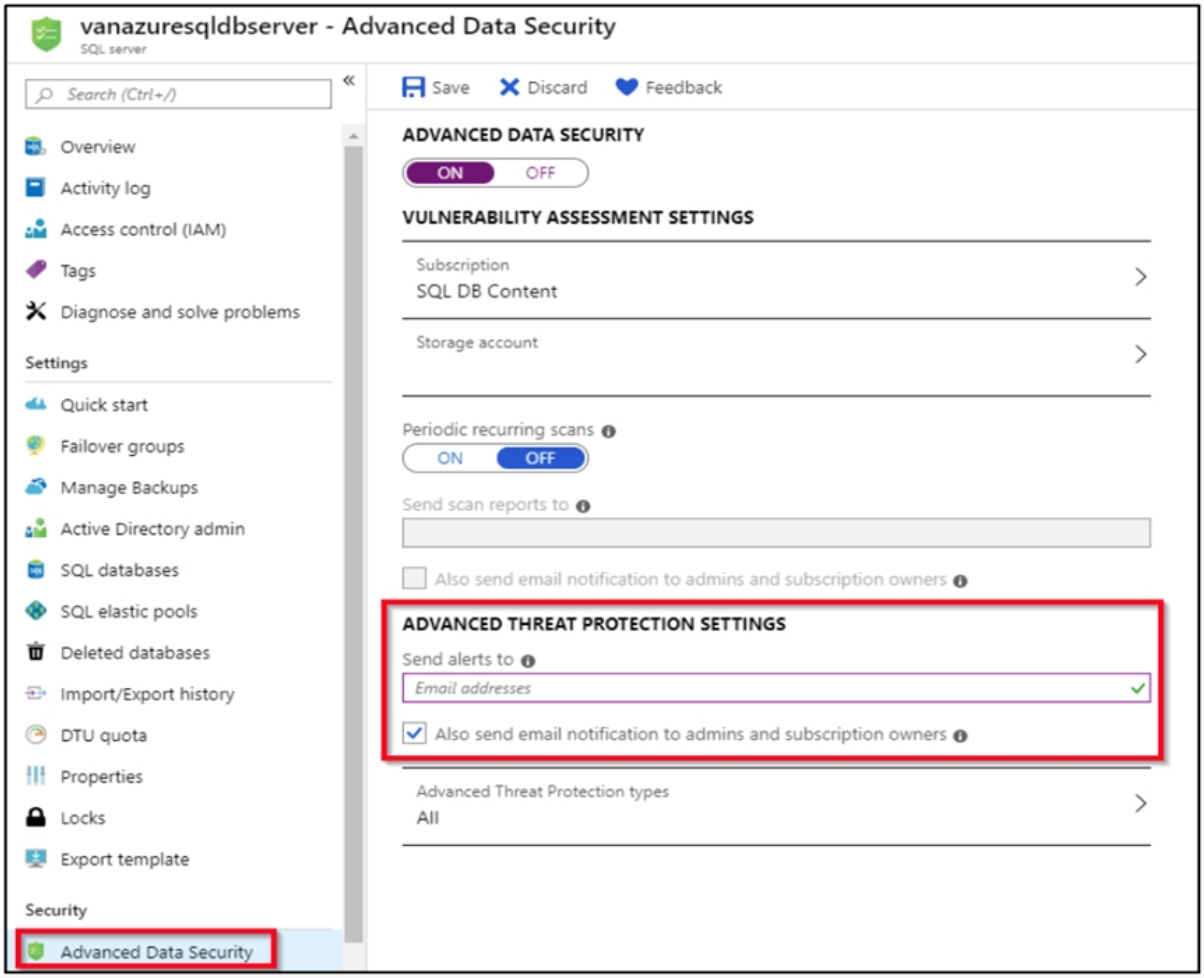
Hide Solution Discussion 4

Correct Answer: *B*
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/
Community vote distribution
B (100%)

Question #32*Topic 4*
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.

Hide Solution Discussion 8

Correct Answer: *See explanation below.*
Set up Advanced Threat Protection in the Azure portal
1. Sign into the Azure portal.
2. Navigate to the configuration page of the server you want to protect. In the security settings, select Advanced Data Security.
3. On the Advanced Data Security configuration page:



4. Enable Advanced Data Security on the server.

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

Reference:

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

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

Question #33*Topic 4*

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

"equals": ▼
- "MicrosoftResources/deployments"
- "MicrosoftResources/subscriptions"
- "MicrosoftResources/subscriptions/resourceGroups"

"effect": ▼
- "Append",
- "Deny",
- "DeployIfNotExists",

Hide Solution | Discussion 63

Correct Answer:

Answer Area

Box 1: " Microsoft.Resources/subscriptions/resourceGroups"
Box 2: "Deny",
Sample - Enforce tag and its value on resource groups
},
"policyRule": {
"if": {
"allOf": [
{
"field": "type",
"equals": "Microsoft.Resources/subscriptions/resourceGroups"
},
{
"not": {
"field": "[concat('tags[',parameters('tagName'), ']')]",
"equals": "[parameters('tagValue')]"
}
}
]
},

```
"then": {
"effect": "deny"
}
}
}
}
```

Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/samples/enforce-tag-on-resource-groups

Question #34*Topic 4*

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.

Hide Solution | Discussion 13

Correct Answer: *B*

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

Community vote distribution

B (100%)

Question #35*Topic 4*

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. **Most Voted**
- B. Modify the Deployment queue settings.
- C. Configure a deployment trigger.
- D. Create a pipeline variable.

Hide Solution | Discussion 10

Correct Answer: *A*

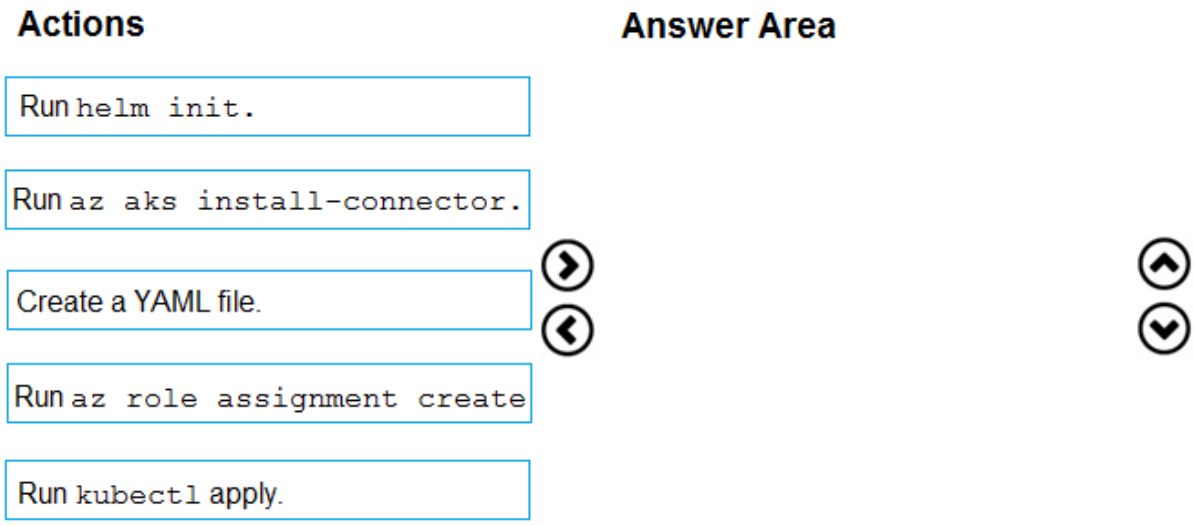
You can check policy compliance with gates.

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 or criteria, without requiring user intervention.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deploy-using-approvals
Community vote distribution

A (100%)

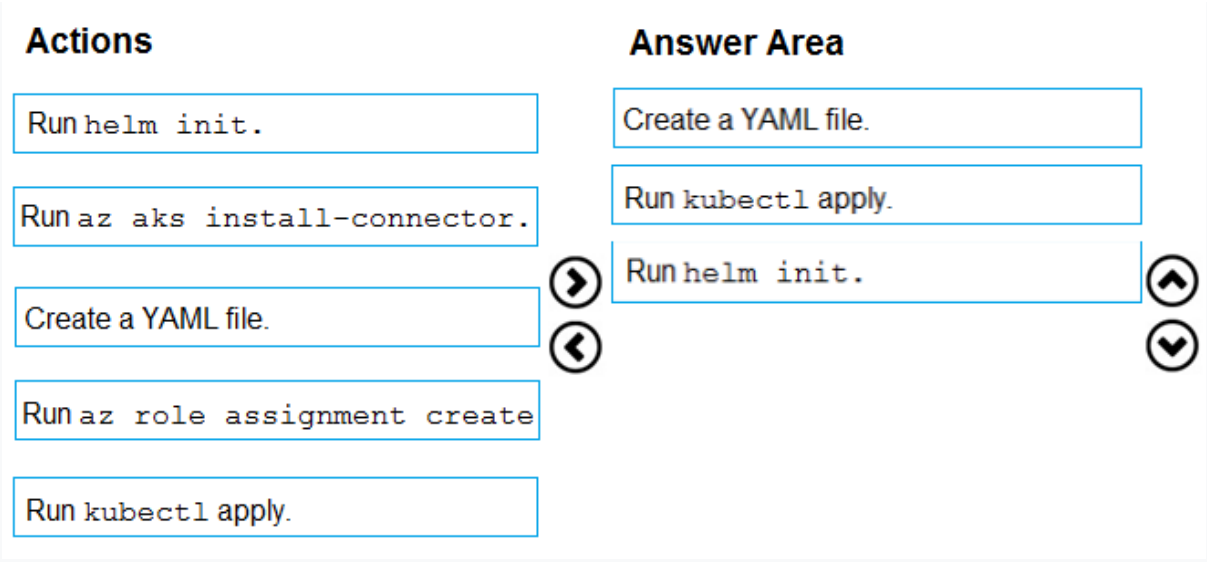
Question #36*Topic 4*

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:



Hide Solution | Discussion 42

Correct Answer:



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

Question #37*Topic 4*

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 **Most Voted**
- D. Helm

Hide Solution | Discussion 5

Correct Answer: *C*
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/
Community vote distribution

C (100%)

Question #38*Topic 4*

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 **Most Voted**

Hide Solution | Discussion 24

Correct Answer: *A*
Incorrect Answers:
B: Jenkins is a popular open-source automation server used to set up continuous integration and delivery (CI/CD) for your software projects.
D: 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.
Reference:
https://octopus.com/docs/packaging-applications
Community vote distribution

D (100%)

Question #39*Topic 4*

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

Hide Solution | Discussion 10

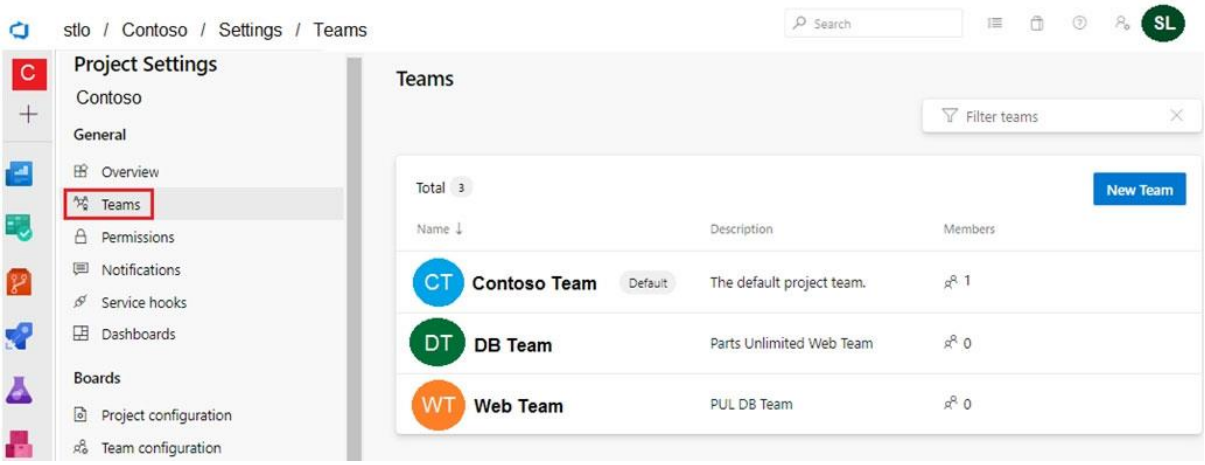
Correct Answer: *B*
Feeds have four levels of access: Owners, Contributors, Collaborators, and Readers. Owners can add any type of identity-individuals, teams, and groups-to any access level.

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				✓

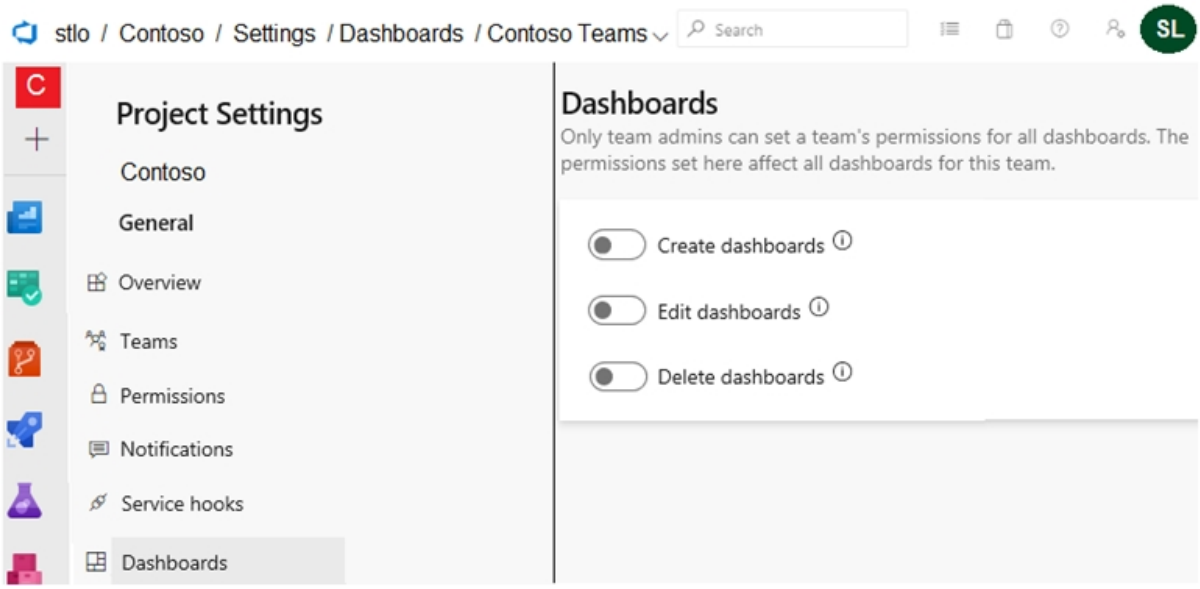
Reference:
https://docs.microsoft.com/en-us/azure/devops/artifacts/feeds/feed-permissions
Community vote distribution
B (100%)

Question #40*Topic 4*

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



You create a new dashboard named Dash1.
You configure the dashboard permissions for the Contoso project as shown in the Permissions exhibit. (Click the Permissions tab.)



All other permissions have the default values set.
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.	○	○

Hide Solution Discussion 9

Correct Answer:

Answer Area

Statements	Yes	No
Web Team can delete Dash1.	○	○
Contoso Team can view Dash1.	○	○
Project administrators can create new dashboards.	○	○

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

Question #41*Topic 4*

Your company is concerned that when developers introduce open source libraries, it creates licensing compliance issues.
You need to add an automated process to the build pipeline to detect when common open source libraries are added to the code base.
What should you use?

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

Hide Solution | Discussion 4

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

Community vote distribution

C (100%)

Question #42*Topic 4*

DRAG DROP -

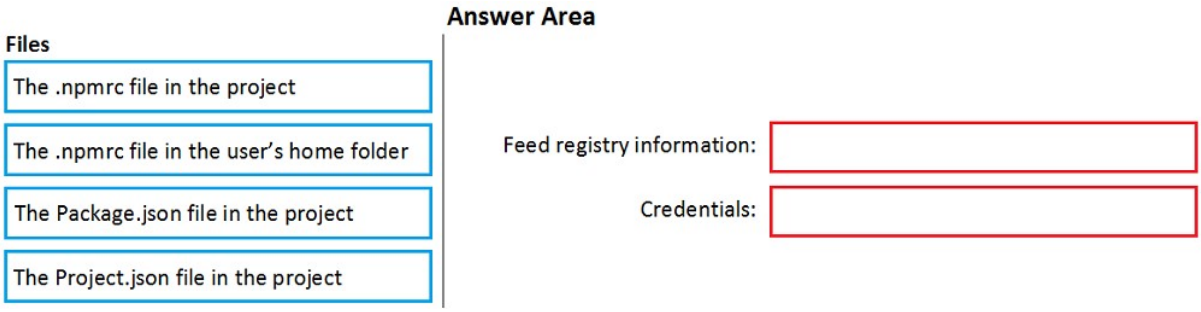
You are implementing a package management solution for a Node.js application by using Azure Artifacts.

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.

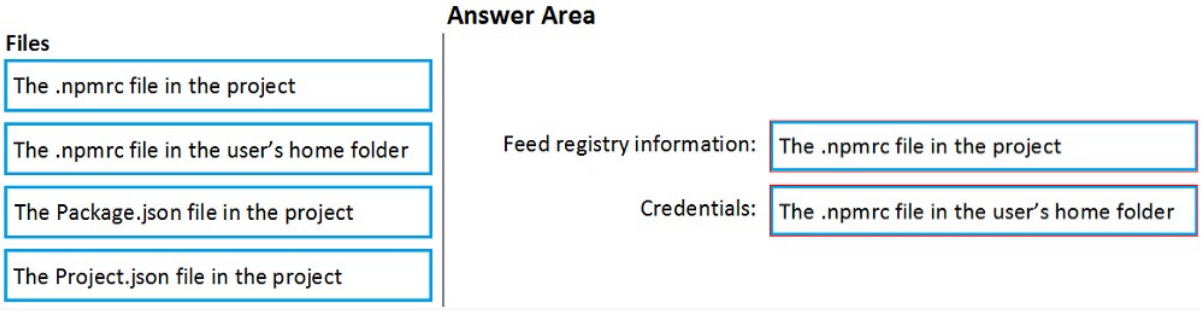
NOTE: Each correct selection is worth one point.

Select and Place:



Hide Solution | Discussion 11

Correct Answer:



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.

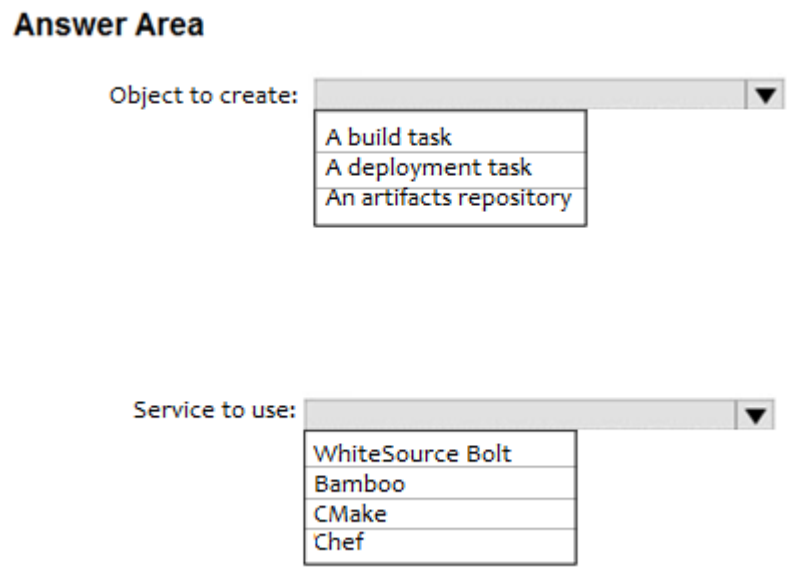
Credentials: The .npmrc file in the user's home folder

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,

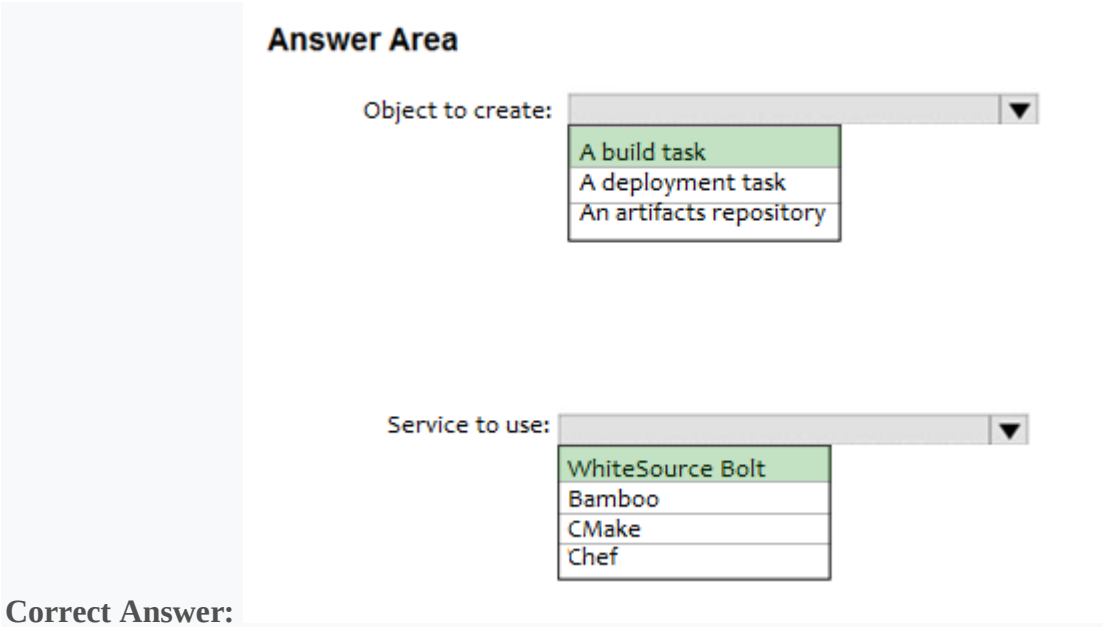
discover the registry, and fetch matching credentials from $home/.npmrc or $env.HOME/.npmrc.
Reference:
https://docs.microsoft.com/en-us/azure/devops/artifacts/npm/npmrc?view=azure-devops&tabs=windows

Question #43*Topic 4*

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:



Hide Solution Discussion 10



Correct Answer:
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 #44*Topic 4*

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

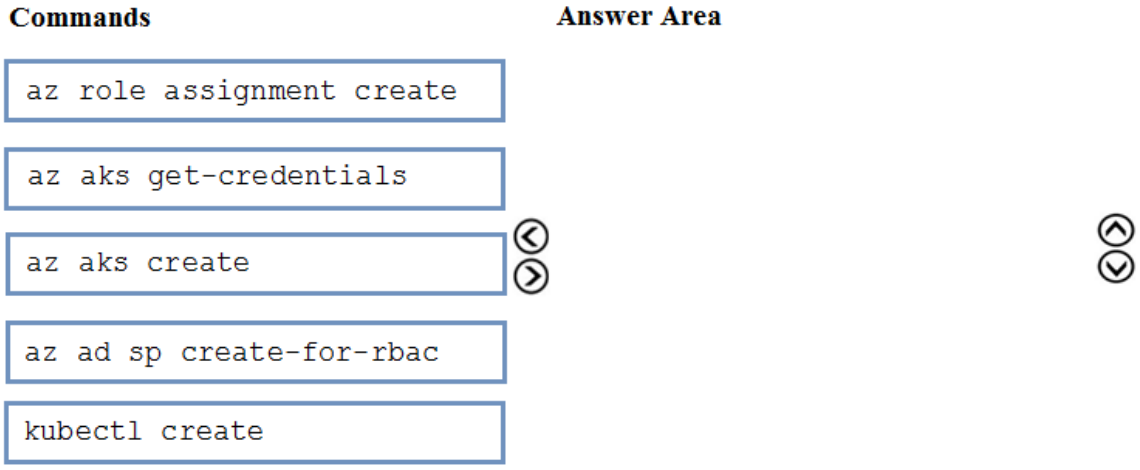
Hide Solution Discussion 7

Correct Answer: *C*
Secure and Manage Open Source Software
Black Duck helps organizations identify and mitigate open source security, license compliance and code-quality risks across application and container portfolios.
Black Duck Hub and its plugin for Team Foundation Server (TFS) allows you to automatically find and fix open source security vulnerabilities during the build process, so you can proactively manage risk. The integration allows you to receive alerts and fail builds when any Black Duck Hub policy violations are met.
Note: WhiteSource would also be a good answer, but it is not an option here.
Reference:
https://marketplace.visualstudio.com/items?itemName=black-duck-software.hub-tfs
Community vote distribution

C (100%)

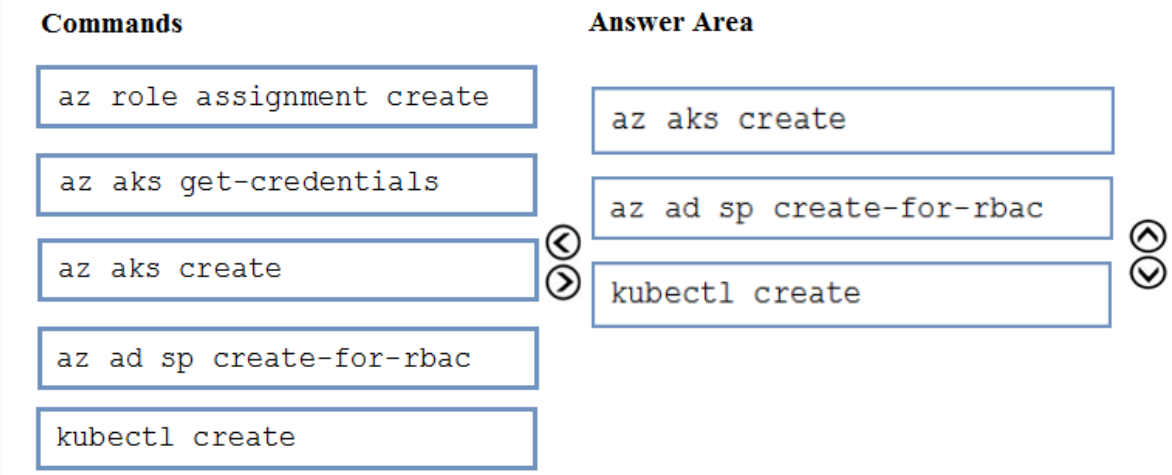
Question #45*Topic 4*

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:



Hide Solution Discussion 39

Correct Answer:



Step 1 : az acr create -
An Azure Container Registry (ACR) can also be created using the new Azure CLI. az acr create
--name <REGISTRY_NAME>
--resource-group <RESOURCE_GROUP_NAME>
--sku Basic
Step 2: az ad sp create-for-rbac
Once the ACR has been provisioned, you can either enable administrative access (which is okay for testing) or you create a Service Principal (sp) which will provide a client_id and a client_secret. az ad sp create-for-rbac
--scopes
/subscriptions/<SUBSCRIPTION_ID>/resourcegroups/<RG_NAME>/providers/Microsoft.ContainerRegistry/registries/<REGISTRY_NAME>
--role Contributor
--name <SERVICE_PRINCIPAL_NAME>

Step 3: kubectl create -
Create a new Kubernetes Secret.
kubectl create secret docker-registry <SECRET_NAME>
--docker-server <REGISTRY_NAME>.azurecr.io
--docker-email <YOUR_MAIL>
--docker-username=<SERVICE_PRINCIPAL_ID>
--docker-password <YOUR_PASSWORD>
Reference:
https://thorsten-hans.com/how-to-use-private-azure-container-registry-with-kubernetes

Question #46*Topic 4*

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 **Most Voted**
- D. .pvk

Hide Solution | Discussion 8

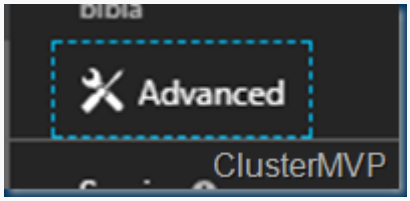
Correct Answer: *C*
A successful IOS device build will produce an ipa file. In order to install the build on a device, it needs to be signed with a valid provisioning profile and certificate.
To sign the builds produced from a branch, enable code signing in the configuration pane and upload a provisioning 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/
Community vote distribution
C (100%)

Question #47*Topic 4*

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.

Hide Solution | Discussion 21

Correct Answer: *See explanation below.*
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

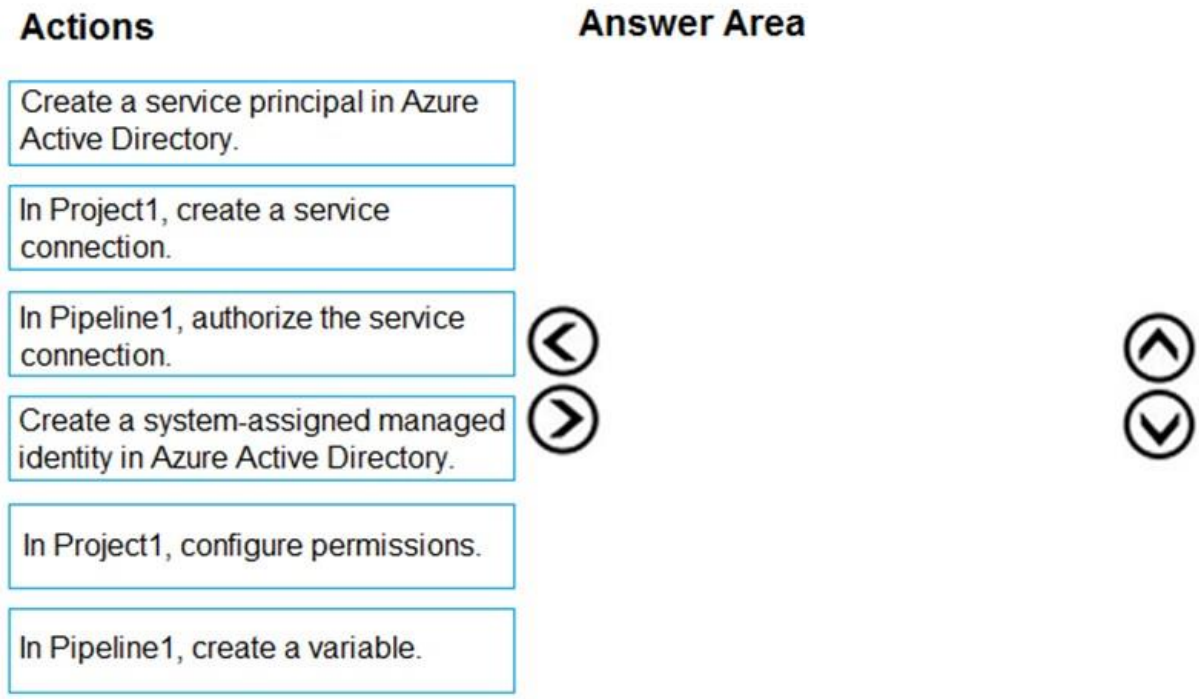


5. Change the following settings:
☞ Destination Port range: 8080
☞ Protocol. TCP
☞ Action: Allow
Note: By default, Azure DevOps Server uses TCP Port 8080.
Reference:
https://robertsmit.wordpress.com/2017/09/11/step-by-step-azure-network-security-groups-nsg-security-center-azure-nsg-network/ https://docs.microsoft.com/en-us/azure/devops/server/architecture/requir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

Question #48*Topic 4*

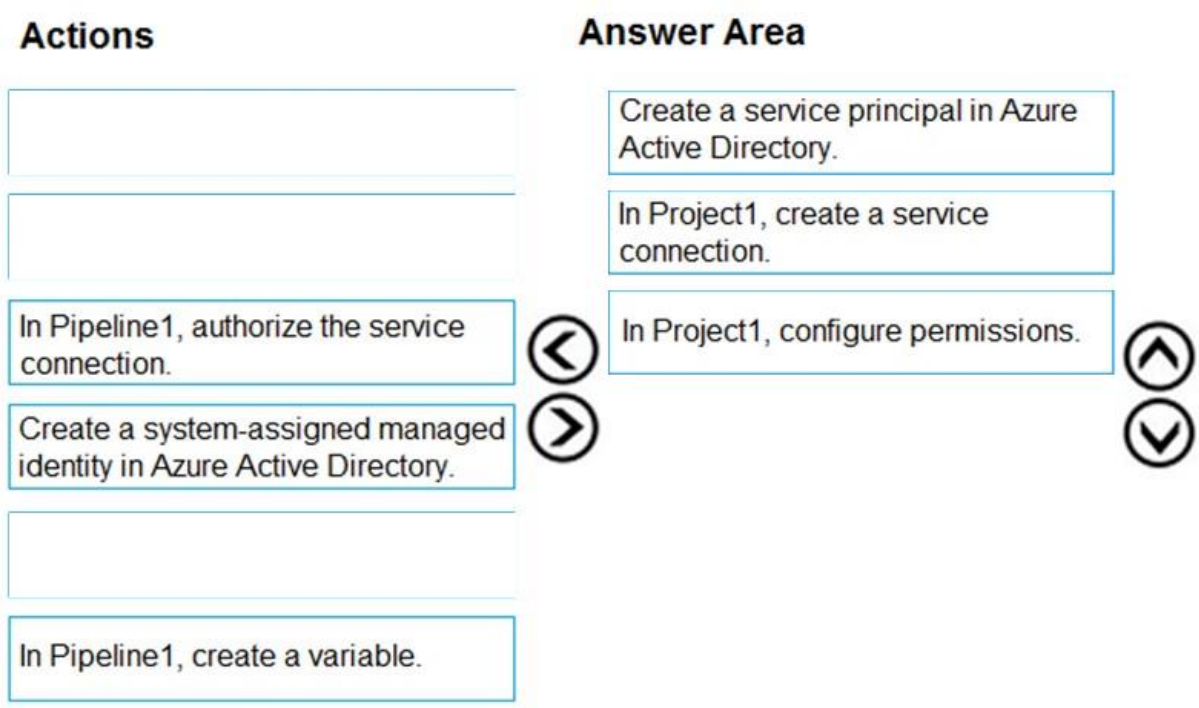
DRAG DROP -
You have a project in Azure DevOps named Project1 that contains two Azure DevOps pipelines named Pipeline1 and Pipeline2.
You need to ensure that Pipeline1 can deploy code successfully to an Azure web app named webapp1. The solution must ensure that Pipeline2 does not have permission to webapp1.

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:



Hide Solution Discussion 13

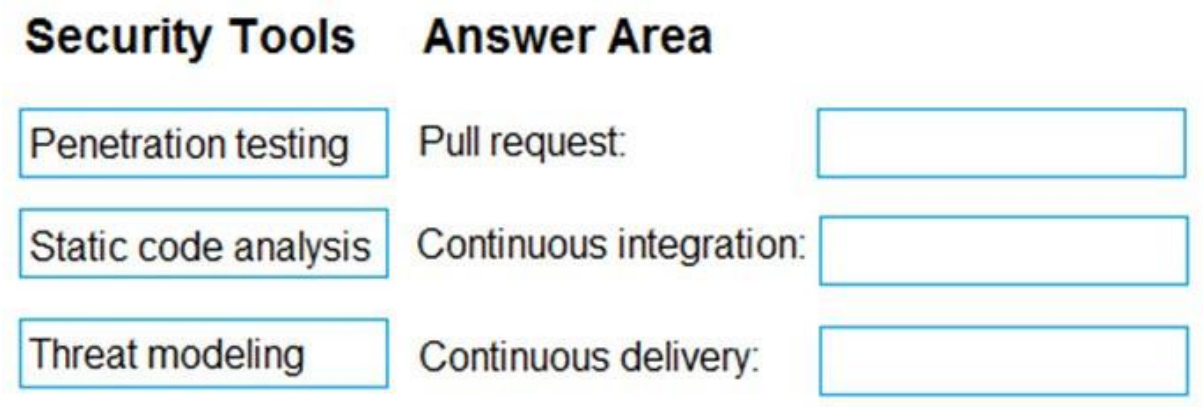
Correct Answer:



Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/library/connect-to-azure?view=azure-devops

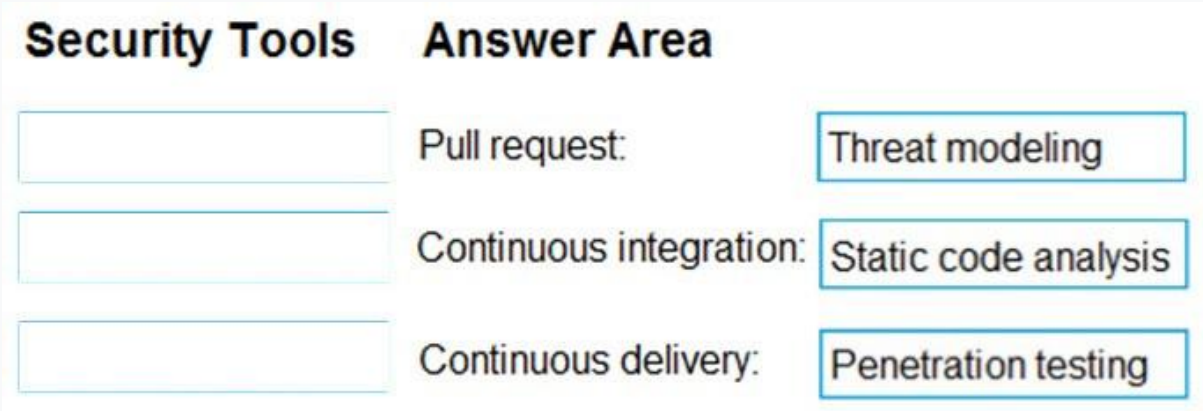
Question #49*Topic 4*

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:



Hide Solution | Discussion 15

Correct Answer:



Box 1: Threat modeling -
Threat modeling's motto should be, ‚€The earlier the better, but not too late and never ignore.‚€
Box 2: Static code analysis -
Validation in the CI/CD begins before the developer commits his or her code. Static code analysis tools in the IDE provide the first line of defense to help ensure that security vulnerabilities are not introduced into the CI/CD process.
Box 3: Penetration testing -
Once your code quality is verified, and the application is deployed to a lower environment like development or QA, the process should verify that there are not any security vulnerabilities in the running application. This can be accomplished by executing automated penetration test against the running application to scan it for vulnerabilities.
Reference:

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

Question #50 *Topic 4*

Your company is concerned that when developers introduce open source libraries, it creates licensing compliance issues.
You need to add an automated process to the build pipeline to detect when common open source libraries are added to the code base.
What should you use?

- A. OWASP ZAP
- B. Jenkins
- C. Code Style
- D. WhiteSource Bolt **Most Voted**

Hide Solution | Discussion 14

Correct Answer: *D*
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/

Community vote distribution

D (100%)

Question #51 *Topic 4*

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 **Most Voted**

- C. an Azure Active Directory (Azure AD) account that has multi-factor authentication (MFA) enabled
- D. an Azure Active Directory (Azure AD) service principal

Hide Solution Discussion 13

Correct Answer: *B*
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
Community vote distribution
B (100%)

Question #52*Topic 4*

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 **Most Voted**
- B. Azure Active Directory Conditional Access Policy Validation
- C. Alternate authentication credentials
- D. SSH authentication

Hide Solution Discussion 11

Correct Answer: *A*
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
Community vote distribution
A (100%)

Question #53*Topic 4*

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 **Most Voted**

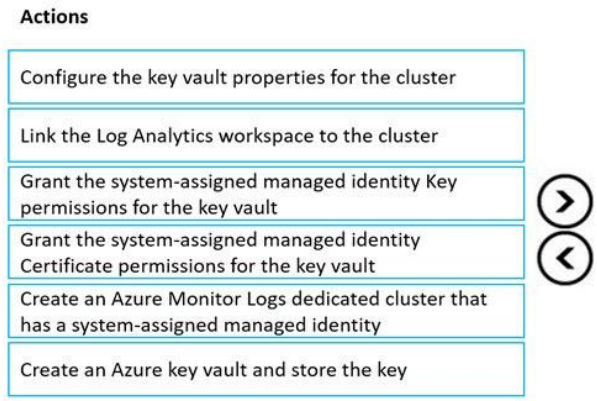
- C. Azure Active Directory (Azure AD)
- D. OAuth

Hide Solution | Discussion 18

Correct Answer: *B*
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
Community vote distribution
B (100%)

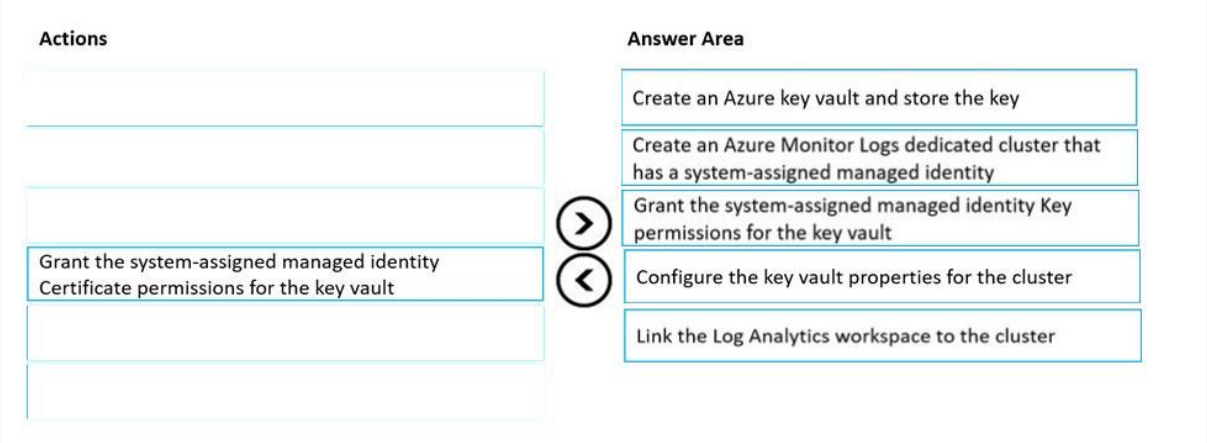
Question #54*Topic 4*

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:

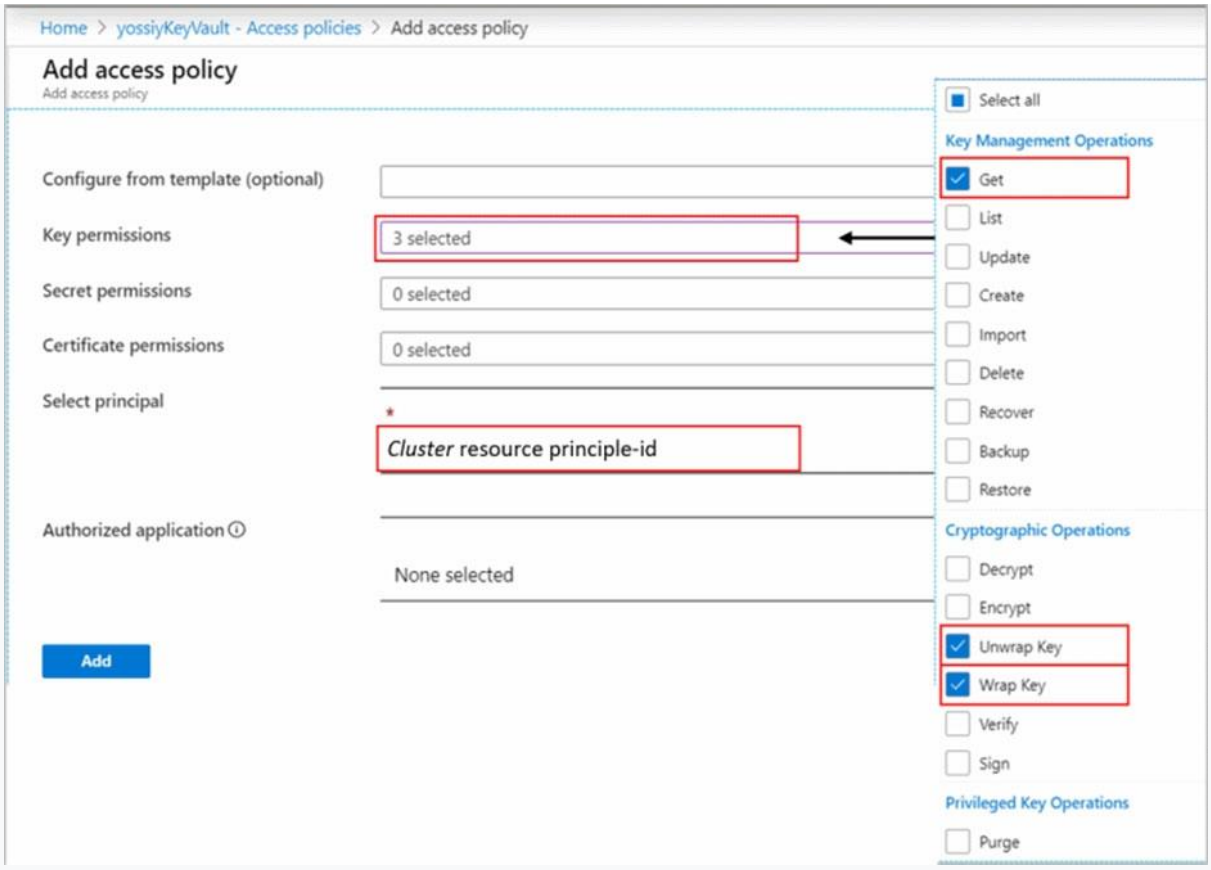


Hide Solution | Discussion 2

Correct Answer:



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 planed, 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.
Etc.

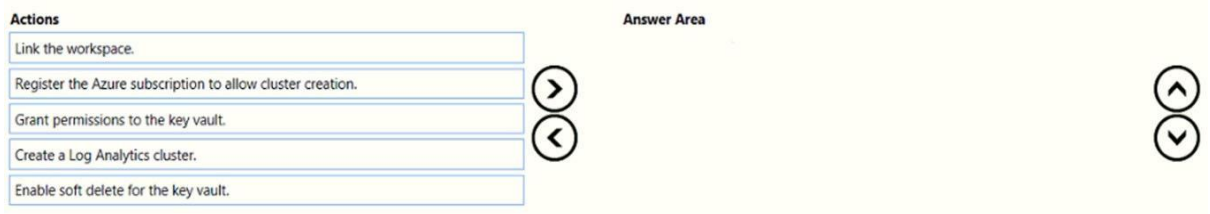


1. Creating cluster
2. Granting permissions to your Key Vault
3. Updating cluster with key identifier details
4. Linking workspaces

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

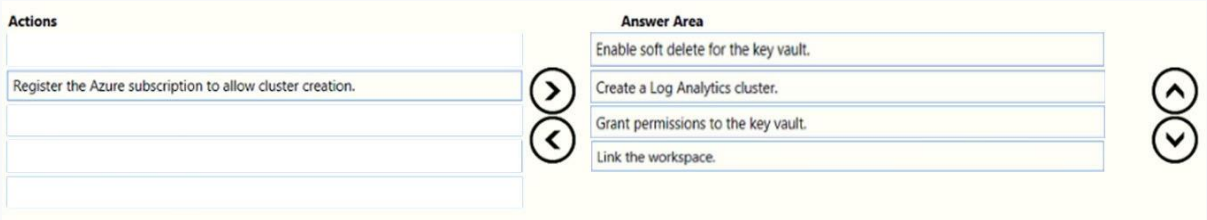
Question #55*Topic 4*

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:

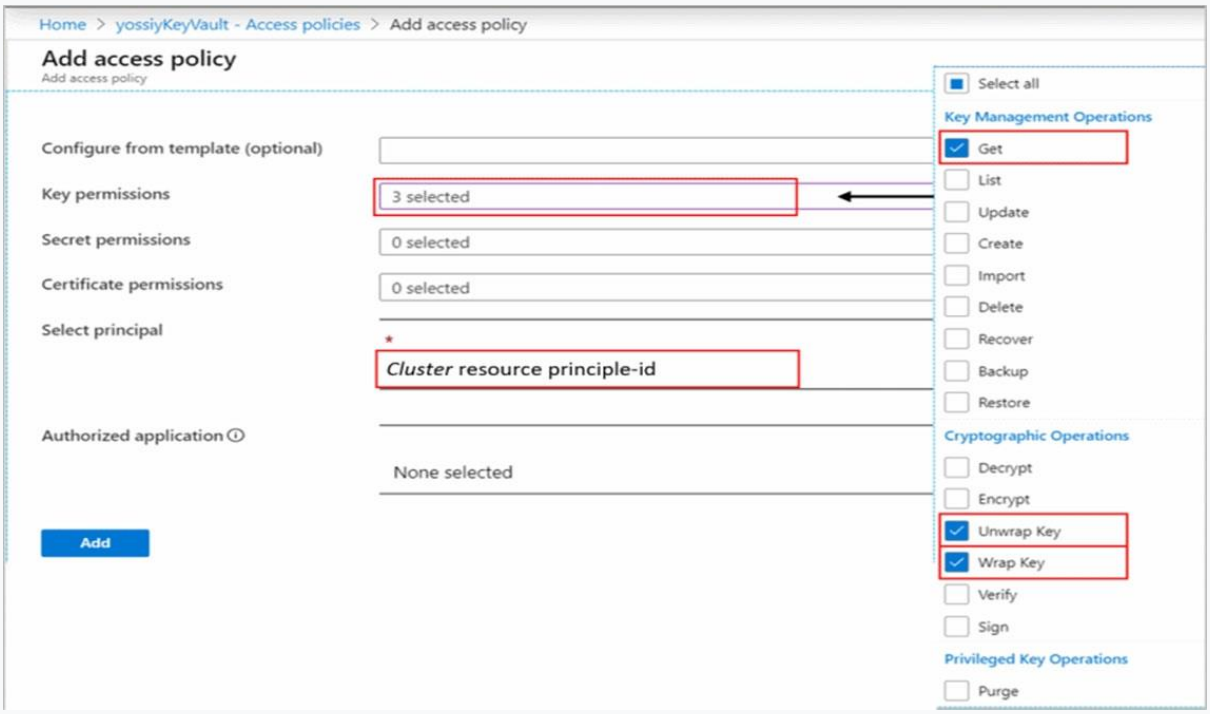


Hide Solution Discussion 7

Correct Answer:



Customer-Managed key provisioning steps (assuming there already is an Azure Key Vault):
Step 1: Enable soft delete for the key vault.
The Azure Key Vault must be configured as recoverable, to protect your key and the access to your data in Azure Monitor. You can verify this configuration under properties in your Key Vault, both Soft delete and Purge protection should be enabled.
Step 2: Create a Log Analytics cluster.
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 permissions to 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 permissionsâ€"select Get, Wrap Key and Unwrap Key.
Etc.



1. Creating cluster
2. Granting permissions to your Key Vault
3. Updating cluster with key identifier details
4. Linking workspaces

Step 4: Link workspace -
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 #56*Topic 4*

You use release pipelines in Azure Pipelines to deploy an app. Secrets required be 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.

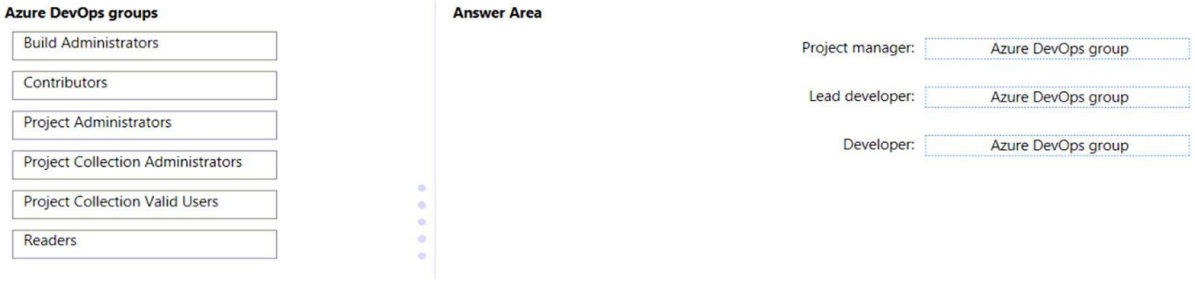
Hide Solution | Discussion 2

Correct Answer: *A*
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
Community vote distribution
A (100%)

Question #57*Topic 4*

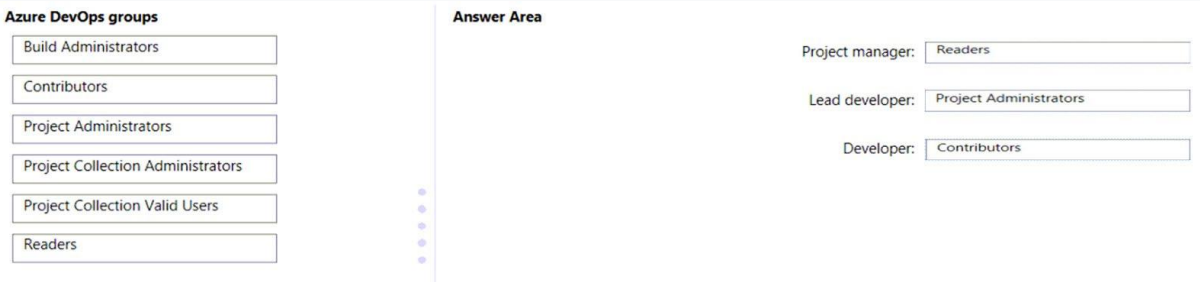
DRAG DROP -
You need to deploy a new project in Azure DevOps that has the following requirements:
* The lead developer must be able to create repositories, manage permissions, manage policies, and contribute to the repository.
* Developers must be able to contribute to the repository and create branches, 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:



Hide Solution Discussion 3

Correct Answer:



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 #58*Topic 4*

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:

Hide Solution Discussion 3

Correct Answer:

Answer Area

User1: Readers

User2: Project Administrators

User3: Contributors

Question #59*Topic 4*

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.

Hide Solution Discussion 2

Correct Answer: *D*

Question #60*Topic 4*

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.

Hide Solution Discussion 3

Correct Answer: *C*

Community vote distribution

D (100%)

Question #61*Topic 4*

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. **Most Voted**
- B. Purchase Premium Plus support.
- C. Enforce multi-factor authentication (MFA).
- D. Create an access policy for secrets.

Hide Solution Discussion 2

Correct Answer: *A*

Community vote distribution

A (100%)

Question #62*Topic 4*

DRAG DROP -

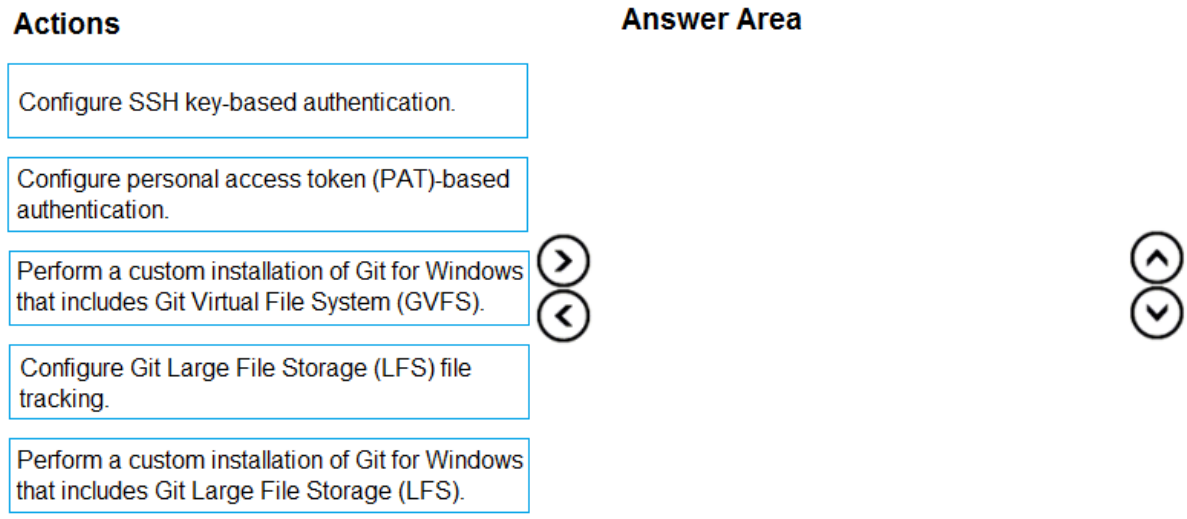
Your company has a project in Azure DevOps named Project1.

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.



Hide Solution Discussion 3

Answer Area

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.

Correct Answer:

5 Topic 5 - Question Set 5

Question #1*Topic 5*

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 **Most Voted**
- D. the JavaScript task runner

Hide Solution | Discussion 12

Correct Answer: *C*
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/
Community vote distribution
C (100%)

Question #2*Topic 5*

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 **Most Voted**
- B. No

Hide Solution | Discussion 17

Correct Answer: *B*
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/
Community vote distribution
A (100%)

Question #3*Topic 5*
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.

Hide Solution | Discussion 24

Correct Answer: *BC*
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/

Community vote distribution

BC (75%)
CD (25%)

Question #4*Topic 5*

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

Hide Solution | Discussion 5

Correct Answer: *A*
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

Community vote distribution

A (100%)

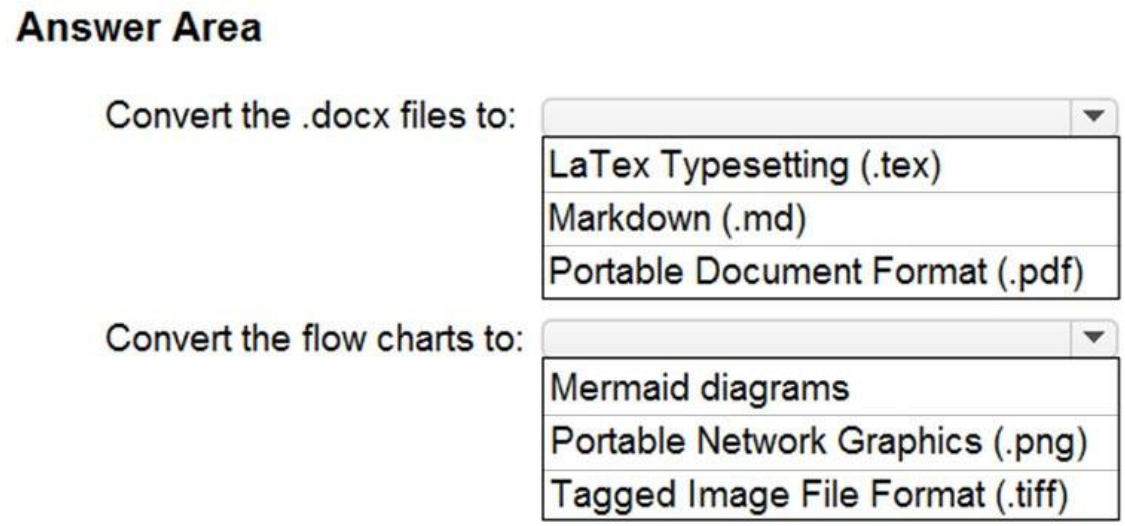
Question #5*Topic 5*

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.

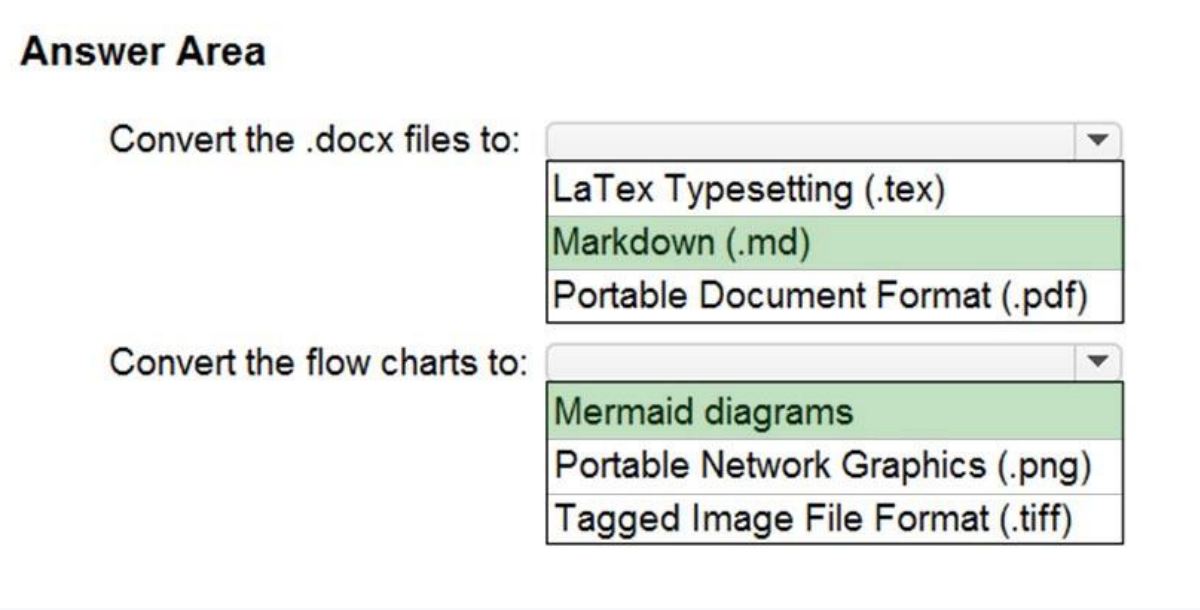
Simplify the modification, merging, and reuse of documents.

▪
Hot Area:



Hide Solution Discussion 2

Correct Answer:



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/#/

Question #6*Topic 5*

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

Hide Solution Discussion 7

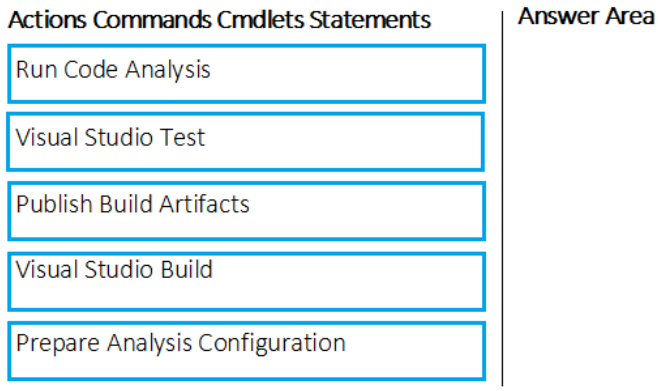
Correct Answer: *C*
SonarQube is a set of static analyzers that can be used to identify areas of improvement in your code. It allows you to analyze the technical debt in your project and keep track of it in the future. With Maven and Gradle build tasks, you can run SonarQube analysis with minimal setup 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
Community vote distribution

C (100%)

Question #7*Topic 5*

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:



Hide Solution Discussion 21

Correct Answer:

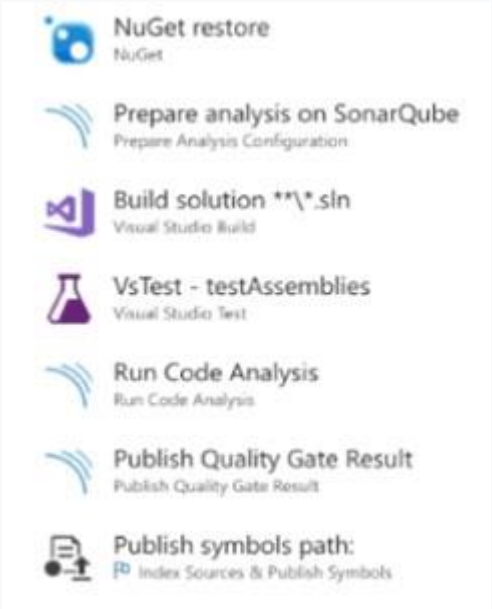
Actions Commands Cmdlets Statements	Answer Area
Run Code Analysis	Prepare Analysis Configuration
Visual Studio Test	Visual Studio Build
Publish Build Artifacts	Visual Studio Test
Visual Studio Build	Run Code Analysis
Prepare Analysis Configuration	

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 #8*Topic 5*

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. **Most Voted**
- C. Integrate Azure DevOps and Azure DevTest Labs.

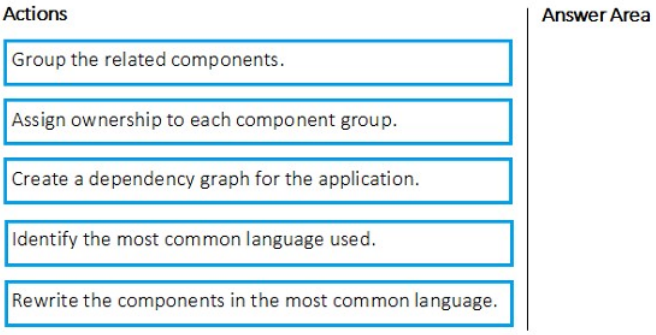
Hide Solution | Discussion 8

Correct Answer: *B*
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/
Community vote distribution
B (100%)

Question #9*Topic 5*

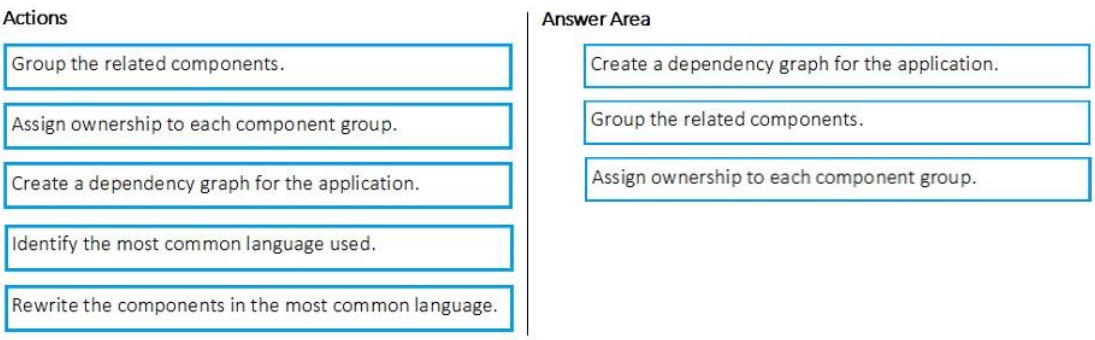
DRAG DROP -
You need to find and isolate shared code. The shared code will be maintained in a series of packages.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Hide Solution Discussion 13

Correct Answer:

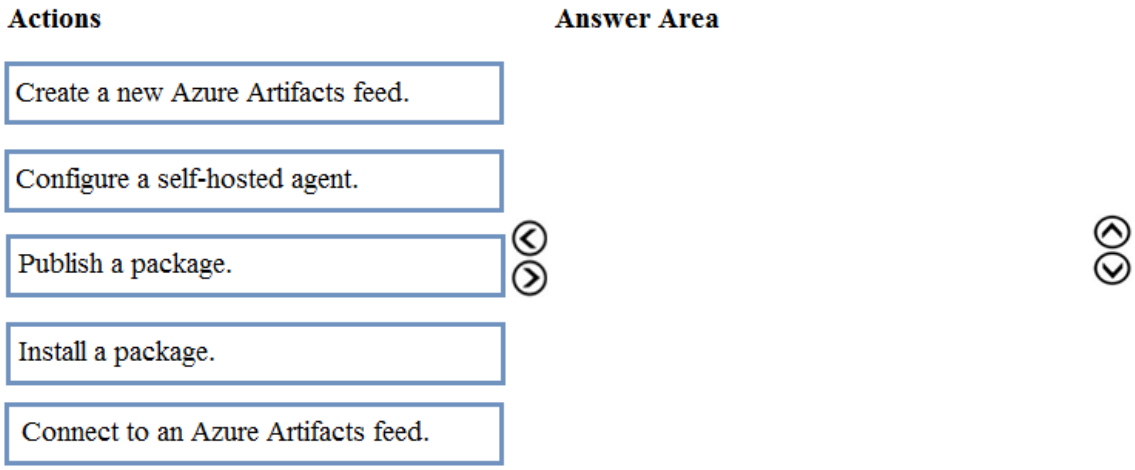


Step 1: Create a dependency graph for the application
By linking work items and other objects, you can track related work, dependencies, and changes made over time. All links are defined with a specific link type. For example, you can use Parent/Child links to link work items to support a hierarchical 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-relnote s

Question #10*Topic 5*

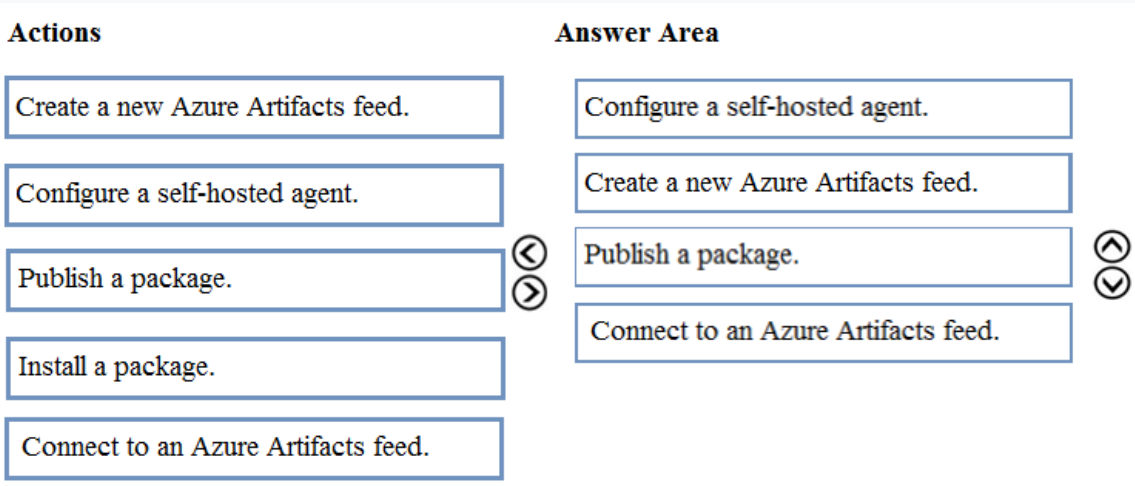
DRAG DROP -
You are creating a NuGet package.
You plan to distribute the package to your development team privately.
You need to share the package and test that the package can be consumed.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions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

Select and Place:



Hide Solution Discussion 37

Correct Answer:



Step 1: Configure a self-hosted agent.
The build will run on a Microsoft hosted agent.
Step 2: Create a new Azure Artifacts feed
Microsoft offers an official extension for publishing and managing your private NuGet feeds.
Step 3: Publish the package.
Publish, pack and push the built project to your NuGet feed.
Step 4: Connect to an Azure Artifacts feed.
With the package now available, you can point Visual Studio to the feed, and download the newly published package
Reference:
https://medium.com/@dan.cokely/creating-nuget-packages-in-azure-devops-with-azure-pipelines-and-yaml-d6fa30f0f15e

Question #11*Topic 5*

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. **Most Voted**
- C. In a Xcode build task, select Use xcpretty from Advanced.
- D. In a Gradle build task, select Run Checkstyle.

Hide Solution | Discussion 11

Correct Answer: *B*
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
/
Community vote distribution
B (100%)

Question #12*Topic 5*

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. **Most Voted**
- B. Create a new feed in Azure Artifacts. **Most Voted**
- 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. **Most Voted**
- F. Create a Git repository in Azure Repos.

Hide Solution | Discussion 12

Correct Answer: *ABE*
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
Community vote distribution

ABE (100%)

Question #13*Topic 5*

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 form 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 **Most Voted**
- B. BFG Repo-Cleaner **Most Voted**
- C. the git rebase command
- D. GitHub Desktop

Hide Solution | Discussion 8

Correct Answer: *AB*
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
Community vote distribution

AB (100%)

Question #14*Topic 5*

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. **Most Voted**

- D. Set Routing algorithm to Round robin.
- E. Set Routing algorithm to Load balance. **Most Voted**

Hide Solution | Discussion 14

Correct Answer: *AE*

A: 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. In this case select the team leader.

E: 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.

Incorrect Answers:

D: The round robin algorithm chooses reviewers based on who's received the least recent review request, focusing on alternating between all members of the team regardless of the number of outstanding reviews they currently have.

Reference:

https://docs.github.com/en/organizations/organizing-members-into-teams/managing-code-review-assignment-for-your-team

Community vote distribution

CE (97%)
3%

Question #15*Topic 5*

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. **Most Voted**
- E. Create a personal access token in Azure DevOps.

Hide Solution | Discussion 19

Correct Answer: *D*

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

Community vote distribution

D (100%)

Question #16*Topic 5*

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 **Most Voted**

Hide Solution | Discussion 12

Correct Answer: *B*
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/

Community vote distribution

B (100%)

Question #17*Topic 5*

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 **Most Voted**
- B. No **Most Voted**

Hide Solution | Discussion 29

Correct Answer: *B*
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/
Community vote distribution

B (60%)
A (40%)

Question #18*Topic 5*

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 **Most Voted**
- B. No

Hide Solution | Discussion 12

Correct Answer: *A*
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/
Community vote distribution

A (100%)

Question #19*Topic 5*

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. **Most Voted**
- 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.

Hide Solution Discussion 16

Correct Answer: *A*
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/
Community vote distribution
A (100%)

Question #20*Topic 5*

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 **Most Voted**
- C. Promote the package to a release view.
- D. Publish the package to a public NuGet repository. **Most Voted**

Hide Solution Discussion 60

Correct Answer: *B*
Azure Artifacts introduces the concept of multiple feeds that you can use to organize and control access to your packages.
Packages you host in Azure Artifacts are stored in a feed. Setting permissions on the feed allows you to share your packages with as many or as few people as your scenario requires.
Feeds have four levels of access: Owners, Contributors, Collaborators, and Readers.
Reference:
https://docs.microsoft.com/en-us/azure/devops/artifacts/feeds/feed-permissions?view=vsts&tabs=new-nav
Community vote distribution
B (61%)
D (36%)
4%

Question #21*Topic 5*

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 **Most Voted**

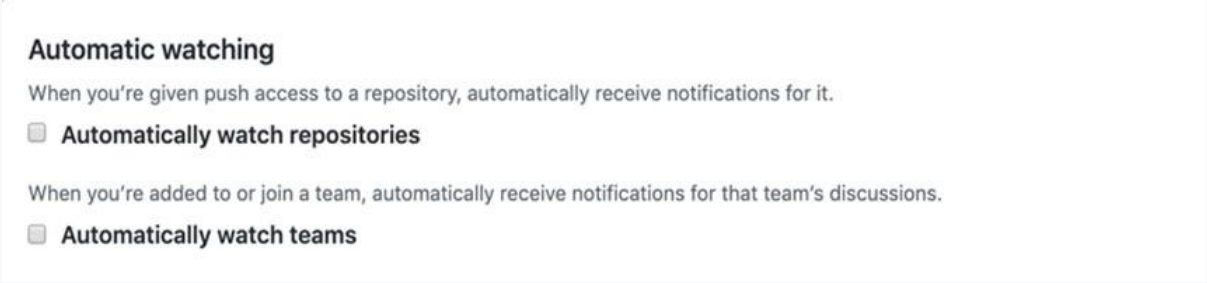
- B. Participating
- C. Automatically watch repositories **Most Voted**
- D. Watching

Hide Solution | Discussion 15

Correct Answer: *BC*

C: If "Automatically watch repositories" is disabled, then you will not automatically watch your own repositories. You must navigate to your repository page and choose the watch option.

A, C: Automatic watching -
By default, anytime you gain access to a new repository, you will automatically begin watching that repository. Anytime you join a new team, you will automatically be subscribed to updates and receive notifications when that team is @mentioned. If you don't want to automatically be subscribed, you can unselect the automatic watching options.



Incorrect:
Not D: When you watch a repository, you're subscribing to updates for activity in that repository. Similarly, when you watch a specific team's discussions, you're subscribing to all conversation updates on that team's page.
Reference:
https://docs.github.com/en/account-and-profile/managing-subscriptions-and-notifications-on-github/setting-up-notifications/configuring-notifications

Community vote distribution

AC (46%)
BD (26%)
AD (20%)
3%

Question #22*Topic 5*

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

Hide Solution Discussion 2

Correct Answer: *C*

Question #23*Topic 5*

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. **Most Voted**
- C. Delete the pull request, and then raise the request again from the default branch.
- D. Update the code in the pull request. **Most Voted**
- E. Add a new workflow for code scanning.

Hide Solution Discussion 9

Correct Answer: *AD*

Community vote distribution

BD (70%)
BC (20%)
10%

Question #24*Topic 5*

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.

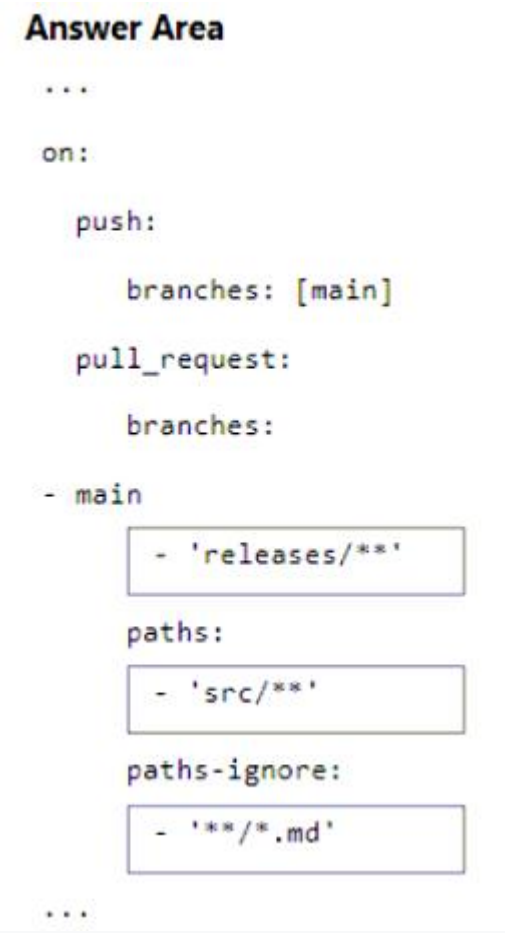
Values

- '**/*.md'
- '*.md'
- 'release*'
- 'releases/**'
- 'src/*'
- 'src/**'

Answer Area

```
...
on:
  push:
     branches: [main]
  pull_request:
     branches:
- main
     [ ]
     paths:
     [ ]
     paths-ignore:
     [ ]
...
```

Hide Solution Discussion 3



Correct Answer:

Question #25*Topic 5*

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

Hide Solution Discussion 1

Correct Answer: *D*

Community vote distribution

D (100%)

Question #26*Topic 5*

DRAG DROP

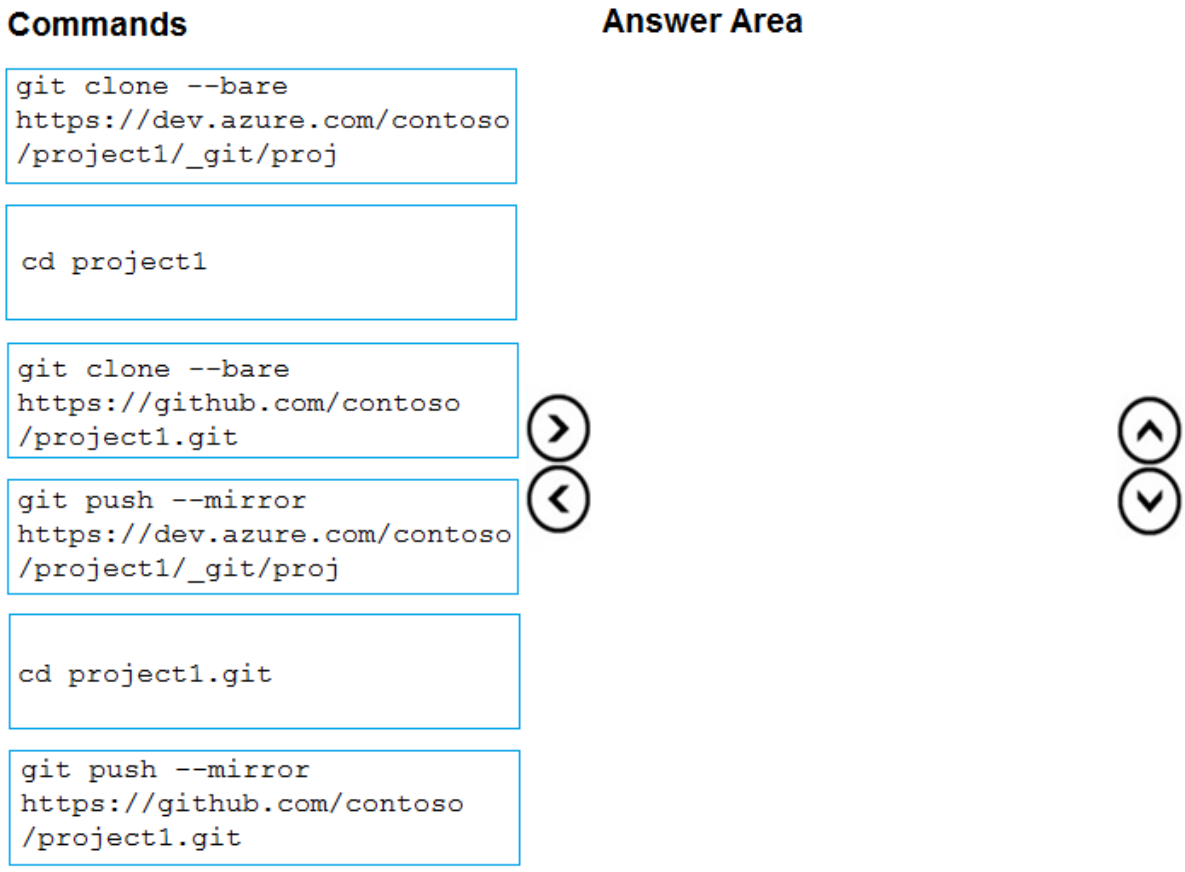
-

You have the repositories shown in the following table.

Type	URL
Azure Repos	https://dev.azure.com/contoso/project1/_git/project1.git
GitHub	https://github.com/contoso/project.git

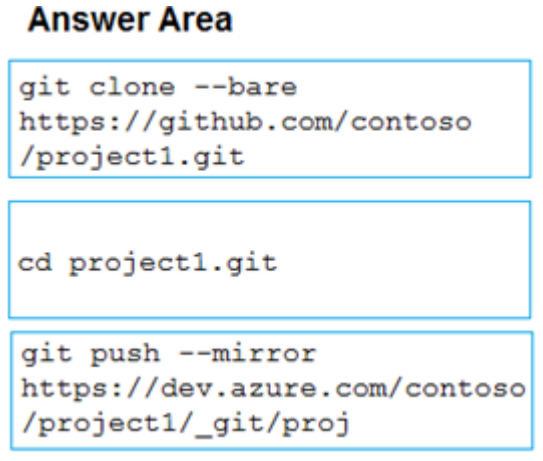
You need to migrate the contents of the GitHub repository to the Azure Repos repository. The solution must ensure that the Azure Repos repository only contains branches and history from the GitHub repository.

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.



Hide Solution Discussion 6

Correct Answer:



Question #27*Topic 5*

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.

Hide Solution Discussion 5

Correct

Answer:

Question #28*Topic 5*

HOTSPOT

-

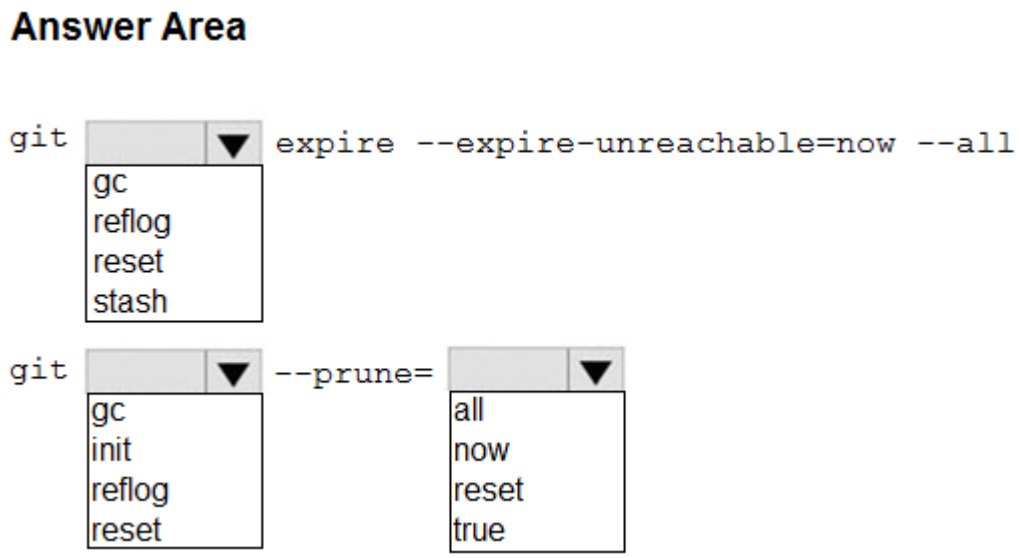
You use Git for source control.

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.

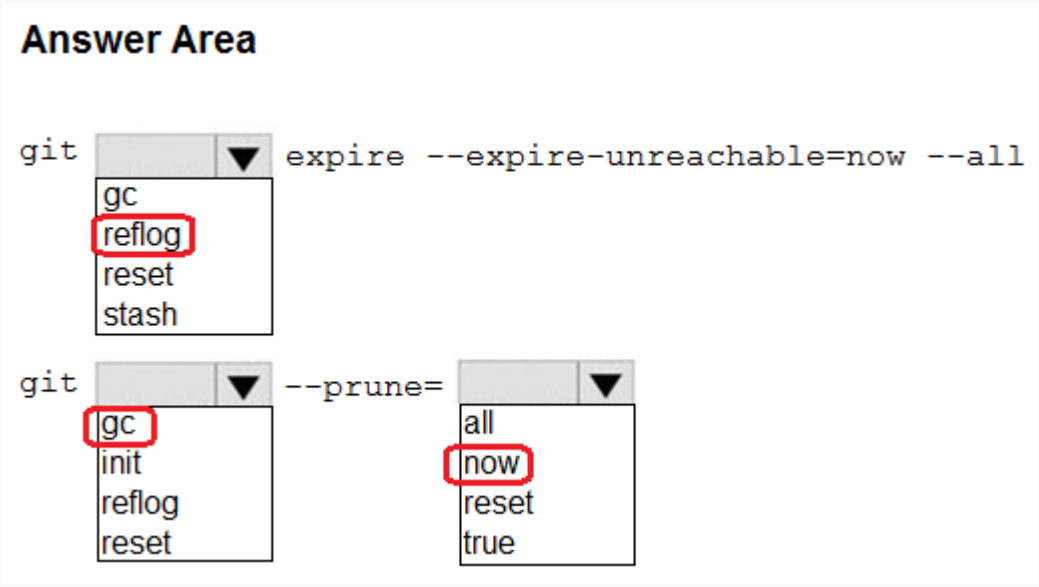
NOTE: Each correct selection is worth one point.



Hide Solution Discussion 2

Correct

Answer:



Question #29*Topic 5*

DRAG DROP

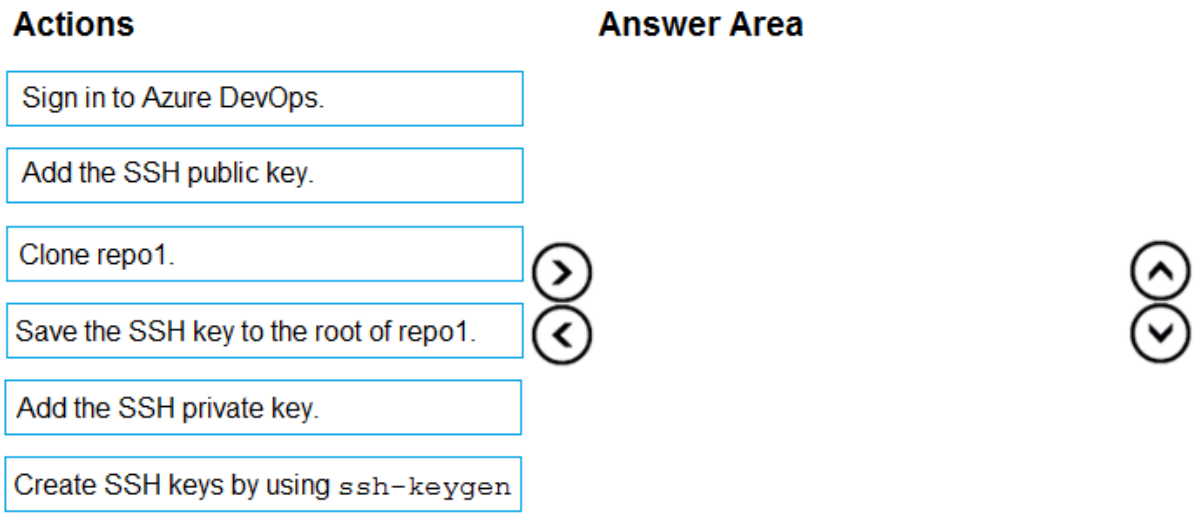
-

You have an Azure Repos Git repository named repo1.

You need to ensure that you can authenticate to repo1 by using SSH.

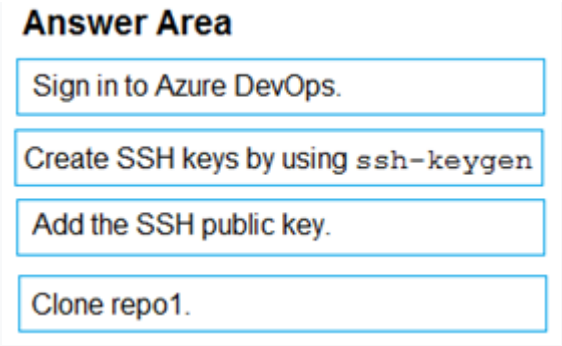
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

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



Hide Solution Discussion 3

Correct Answer:



Question #30 *Topic 5*

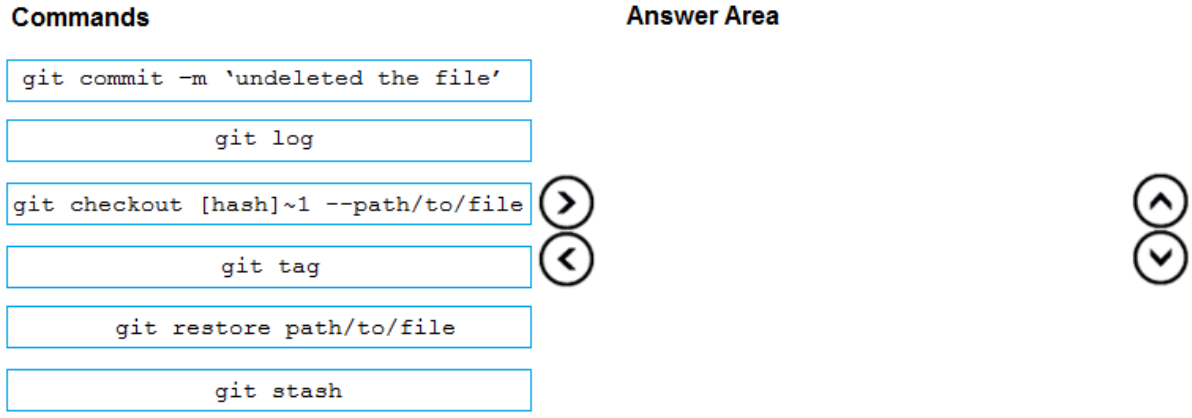
DRAG DROP
-

You use Git for source control.

You delete a file, commit the changes, and continue to work.

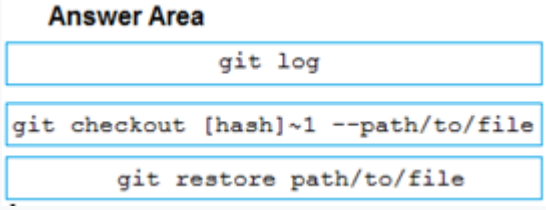
You need to recover the deleted file.

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.



Hide Solution Discussion 6

Correct Answer:



Question #31 *Topic 5*

HOTSPOT
-

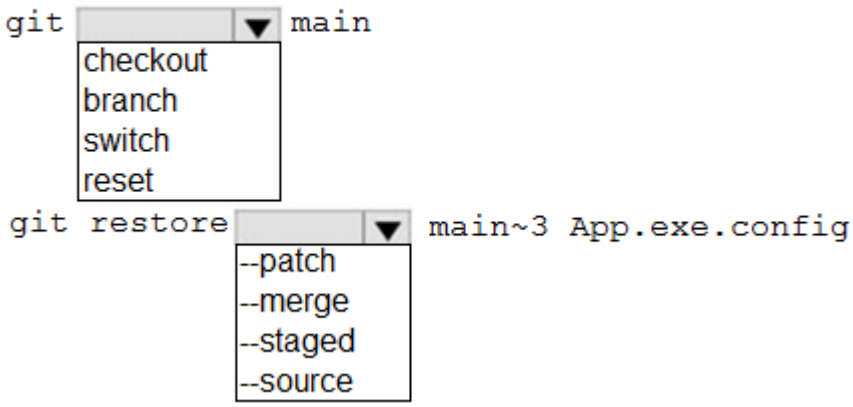
You use Git for source control. You have an app named App1.

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.

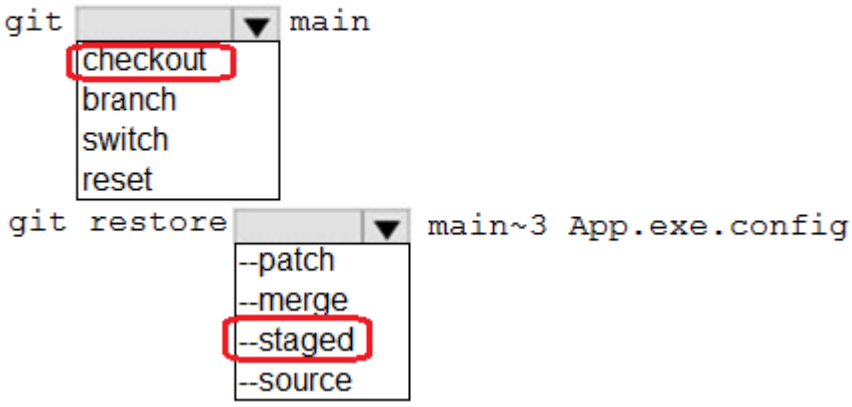
NOTE: Each correct selection is worth one point.

Answer Area



Hide Solution Discussion 3

Answer Area



Correct Answer:

Question #32*Topic 5*

HOTSPOT

-

You company uses a Git source-code repository.

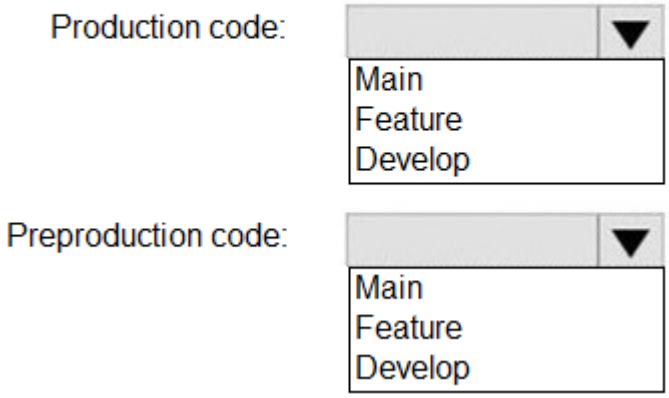
You plan to implement GitFlow as a workflow strategy.

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.

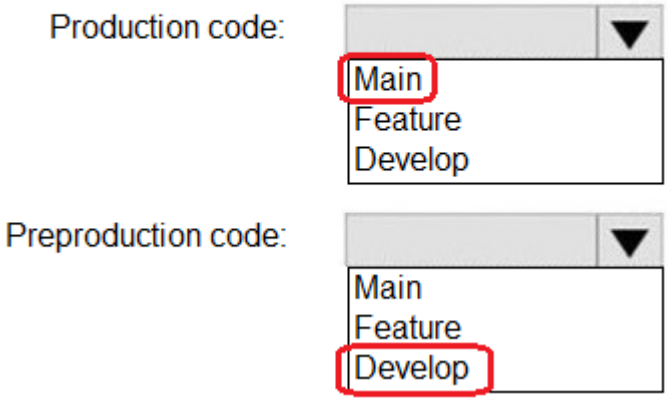
Answer Area



Hide Solution Discussion 2

Correct Answer:

Answer Area



6 Topic 6 - Question Set 6

Question #1*Topic 6*

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 **Most Voted**

Hide Solution | Discussion 6

Correct Answer: *A*
A feature typically represents a shippable component of software.
Features, examples:
- Add view options to the new work hub
- Add mobile shopping cart
- Support text alerts
- Refresh the web portal with new look and feel

User Stories and Tasks are used to track work. Teams can choose how they track bugs, either as requirements or as tasks
Incorrect Answers:
B, C: An epic represents a business initiative to be accomplished.
Epics, examples:
- Increase customer engagement
- Improve and simplify the user experience
- Implement new architecture to improve performance
- Engineer the application to support future growth
- Support integration with external services

Support mobile apps -
▪
Reference:
https://docs.microsoft.com/en-us/azure/devops/boards/backlogs/define-features-epics
https://docs.microsoft.com/en-us/azure/devops/boards/work-items/about-work-items
Community vote distribution
D (88%)
12%

Question #2*Topic 6*
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 **Most Voted**
- B. sprint planning
- C. delivery plans
- D. portfolio backlogs

Hide Solution Discussion 12

Correct Answer: *A*

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/

Community vote distribution

A (100%)

Question #3*Topic 6*

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? **Most Voted**
- D. What went well? **Most Voted**
- E. What should we try next? **Most Voted**

Hide Solution Discussion 47

Correct Answer: *BCE*

Sprint retrospective meetings -

The sprint retrospective meeting typically occurs on the last day of the sprint, after the sprint review meeting. In this meeting, your team explores its execution of

Scrum and what might need tweaking.

Based on discussions, your team might decide to change one or more processes to improve its own effectiveness, productivity, quality, and satisfaction. This meeting and the resulting improvements are critical to the agile principle of self-organization.

Look to address these areas during your team sprint retrospectives:

☞ Issues that affected your team's general effectiveness, productivity, and quality.

☞ Elements that impacted your team's overall satisfaction and project flow.

☞ What happened to cause incomplete backlog items? What actions will the team take to prevent these issues in the future?

Reference:

https://docs.microsoft.com/en-us/azure/devops/boards/sprints/best-practices-scrum

Community vote distribution

CDE (100%)

Question #4*Topic 6*

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 **Most Voted**

Hide Solution | Discussion 10

Correct Answer: *D*
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
Community vote distribution
D (100%)

Question #5*Topic 6*

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

Hide Solution | Discussion 14

Correct Answer: *B*
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.
Community vote distribution
B (100%)

Question #6*Topic 6*

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

Hide Solution Discussion 5

Correct Answer: *D*
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/
Community vote distribution
D (100%)

Question #7*Topic 6*
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 **Most Voted**

Hide Solution Discussion 4

Correct Answer: *D*
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
Community vote distribution
D (100%)

Question #8*Topic 6*

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 **Most Voted**

Hide Solution | Discussion 16

Correct Answer: *B*
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
Community vote distribution
B (83%)
A (17%)

Question #9*Topic 6*

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 **Most Voted**
- B. No

Hide Solution Discussion 10

Correct Answer: *A*

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

Community vote distribution

A (100%)

Previous QuestionsNext Questions