

Microsoft.AZ-400.LAB.vMay-2024.by.Ancher.126q

Number: AZ-400
Passing Score: 800
Time Limit: 120
File Version: 12.0

Exam Code: AZ-400
Exam Name: Microsoft Azure DevOps Solutions



01 - Develop an instrumentation strategy

QUESTION 1

You have an Azure DevOps project named Project1 and an Azure subscription named Sub1. Sub1 contains an Azure virtual machine scale set named VMSS1. VMSS1 hosts a web application named WebApp1. WebApp1 uses stateful sessions.

The WebApp1 installation is managed by using the Custom Script extension. The script resides in an Azure Storage account named sa1. You plan to make a minor change to a UI element of WebApp1 and to gather user feedback about the change. You need to implement limited user testing for the new version of WebApp1 on VMSS1.

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

NOTE: Each correct selection is worth one point.

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

Correct Answer: B, C, D

Section:

QUESTION 2

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

The screenshot shows the 'Create rule' interface in Azure Monitor. It is divided into three main sections: RESOURCE, CONDITION, and ACTIONS GROUPS (optional).
- **RESOURCE:** Shows the resource 'ASP-9bb7' with a 'Select' button.
- **CONDITION:** Shows a condition: 'Whenever the Activity Log has an event with Category='Administrative', Signal name='All Administrative operations', Status='Failed''. There is an 'Add' button below it.
- **ACTIONS GROUPS (optional):** Shows an action group named 'Application Insights Smart Detection' with the action '2 Email Azure Resource Manager Role(s)'. There are 'Add' and 'Create' buttons below it.
There are also two informational banners: one about Azure Alerts limits and another about Action rules (preview).

Which action will trigger an alert?

- A. a failed attempt to delete the ASP-9bb7 resource
- B. a change to a role assignment for the ASP-9bb7 resource

- C. a successful attempt to delete the ASP-9bb7 resource
- D. a failed attempt to scale up the ASP-9bb7 resource

Correct Answer: A

Section:

QUESTION 3

You have a web app hosted on Azure App Service. The web app stores data in an Azure SQL database.

You need to generate an alert when there are 10,000 simultaneous connections to the database. The solution must minimize development effort. Which option should you select in the Diagnostics settings of the database?

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

Correct Answer: A

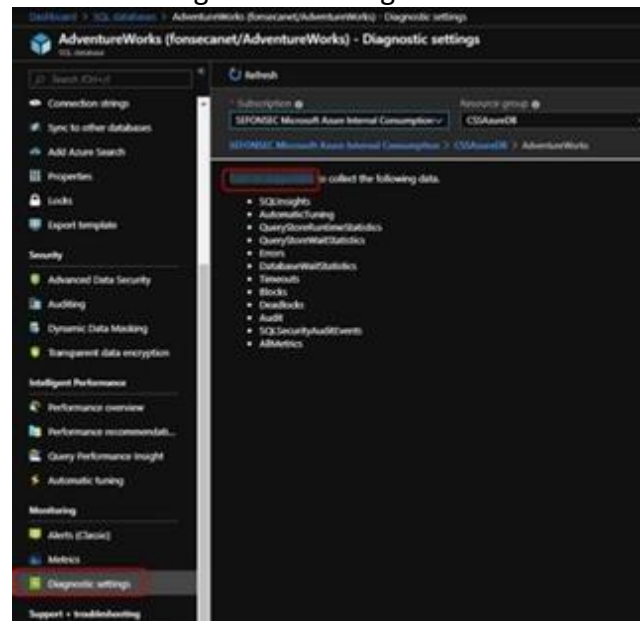
Section:

Explanation:

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

The logo for 'Vdumps' features a stylized orange 'V' followed by the word 'dumps' in a grey, sans-serif font.



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

QUESTION 4
DRAG DROP
You need to recommend project metrics for dashboards in Azure DevOps.
Which chart widgets should you recommend for each metric? To answer, drag the appropriate chart widgets to the correct metrics. Each chart widget may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Select and Place:

Chart Widgets

Answer Area

Burndown

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

Cycle Time

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

Lead Time

The remaining work:

Velocity

Correct Answer:

Chart Widgets

Answer Area

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

Lead Time

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

Cycle Time

Velocity

The remaining work:

Burndown

Section:

Explanation:

Box 1: Lead time

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

Box 2: Cycle time

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

Box 3: Burndown

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

Incorrect Answers:

Velocity provides a useful metric for these activities:

Support sprint planning

Forecast future sprints and the backlog items that can be completed

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

References:

<https://docs.microsoft.com/en-us/azure/devops/report/dashboards/velocity-guidance?view=vsts>

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

<https://docs.microsoft.com/en-us/azure/devops/report/dashboards/configure-burndown-burndown-widgets?view=vsts>

QUESTION 5

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.



Application Insights Demo > Analytics

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

Demo

Run Time range: Set in query

```

requests
| where timestamp >= ago(7d)
| where operation_Name endswith( 'Home/Index' )
| where operation_Name startswith( 'GET' )
| summarize percentiles(duration, 50, 90, 95) by bin(timestamp, 1h)
| extend threshold=675
| render timechart
  
```

Completed 00:00:00.449 169 records

TABLE CHART Line Timestamp 4 Selected Sum Display Time (UTC+00:00)

Legend =>

- percentile_duration_50
- percentile_duration_90
- percentile_duration_95
- threshold

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

Hot Area:

Answer Area

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

	▼
percentile_duration_50	
percentile_duration_90	
percentile_duration_95	
threshold	

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

	▼
item Type	
resultCode	
source	
success	

Answer 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	

Section:

Explanation:

Box 1: percentile_duration_95

Box 2: resultCode

Reference:

<https://devblogs.microsoft.com/premier-developer/alerts-based-on-analytics-query-using-custom-log-search/>

QUESTION 6

HOTSPOT

You have an Azure Kubernetes Service (AKS) pod.

You need to configure a probe to perform the following actions:

Confirm that the pod is responding to service requests.

Check the status of the pod four times a minute.

Initiate a shutdown if the pod is unresponsive.

How should you complete the YAML configuration file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
apiVersion: v1
kind: Pod
metadata:
  labels:
    test: readiness-and-liveness
  name: readiness-http
spec:
  containers:
  - name: container1
    image: k8s.gcr.io/readiness-and-liveness
    args:
    - /server
```

	▼
livenessProbe:	
readinessProbe:	
ShutdownProbe:	
startupProbe:	

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

	▼
initialDelaySeconds: 15	
periodSeconds: 15	
timeoutSeconds: 15	

Answer 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	



Section:

Explanation:

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 7

HOTSPOT

Your company is building a new web application.

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

All the pilot users have a corporate computer that has Google Chrome and the Microsoft Test & Feedback extension installed. The pilot users will test the application by using Chrome. You need to identify which access levels are required to ensure that developers can request and gather feedback from the pilot users. The solution must use the principle of least privilege. Which access levels in Azure DevOps should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Developers:

Pilot users:

Answer Area:

Answer Area

Developers:

Pilot users:



Section:

Explanation:

Box 1: Basic

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

Box 2: Stakeholder

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

Note:

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

Basic: provides access to most features

VS Enterprise: provides access to premium features

Stakeholders: provides partial access, can be assigned to unlimited users for free
References: <https://docs.microsoft.com/en-us/azure/devops/organizations/security/access-levels?view=vsts>

QUESTION 8
DRAG DROP

Your company wants to use Azure Application Insights to understand how user behaviors affect an application. Which application Insights tool should you use to analyze each behavior? To answer, drag the appropriate tools to the correct behaviors. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Select and Place:

Tools	Answer Area
Impact	Feature usage:
User Flows	User actions by day:
Users	The effect that the performance of the application has on the usage of a page or a feature:

Correct Answer:

Tools	Answer Area
	Feature usage: User Flows
	User actions by day: Users
	The effect that the performance of the application has on the usage of a page or a feature: Impact

Section:
Explanation:

Box 1: User Flows

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

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

What do users click on a page on your site?

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

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

Box 2: Users

Box 3: Impact

Reference:

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

QUESTION 9

SIMULATION

You need to create a notification if the peak average response time of an Azure web app named az400-9940427-main is more than five seconds when evaluated during a five-minute period. The notification must trigger the "https://contoso.com/notify" webhook.

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

A. See solution below.

Correct Answer: A

Section:

Explanation:

1. Open Microsoft Azure Portal

2. Log into your Azure account and go to App Service and look under Monitoring then you will see Alert. 3. Select Add an alert rule

4. Configure the alert rule as per below and click Ok.

Source: Alert on Metrics

Resource Group: az400-9940427-main

Resource: az400-9940427-main

Threshold: 5

Period: Over the last 5 minutes

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

The logo for Vdumps.com, featuring a stylized orange 'V' followed by the word 'dumps' in a grey, lowercase, sans-serif font.

Add an alert rule

* Threshold ⓘ
1 bytes/second

* Period ⓘ
Over the last 5 minutes

Email service and co-administrators

Additional administrator email
Additional administrator email

Webhook ⓘ
HTTP or HTTPS endpoint to route alerts to
[Learn more about configuring webhooks](#)

OK

Reference:

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



QUESTION 10

SIMULATION

You need to create and configure an Azure Storage account named az400lod11566895stor in a resource group named RG1lod11566895 to store the boot diagnostics for a virtual machine named VM1. To complete this task, sign in to the Microsoft Azure portal.

A. See solution below.

Correct Answer: A

Section:

Explanation:

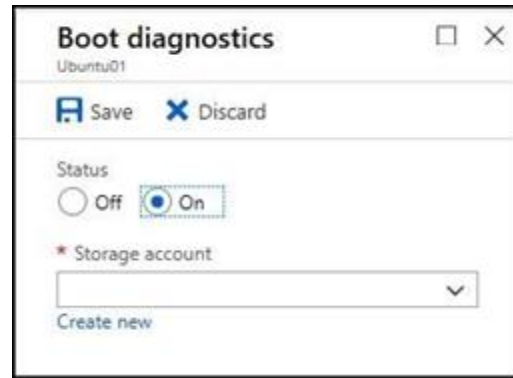
Step 1: To create a general-purpose v2 storage account in the Azure portal, follow these steps:

1. On the Azure portal menu, select All services. In the list of resources, type Storage Accounts. As you begin typing, the list filters based on your input. Select Storage Accounts.
2. On the Storage Accounts window that appears, choose Add.
3. Select the subscription in which to create the storage account.
4. Under the Resource group field, select RG1lod11566895
5. Next, enter a name for your storage account named: az400lod11566895stor
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 az400lod11566895stor.
4. Save the change.



You must restart the virtual machine for the change to take effect.

Reference:

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

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/boot-diagnostics>

QUESTION 11

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.

A. See solution below.

Correct Answer: A

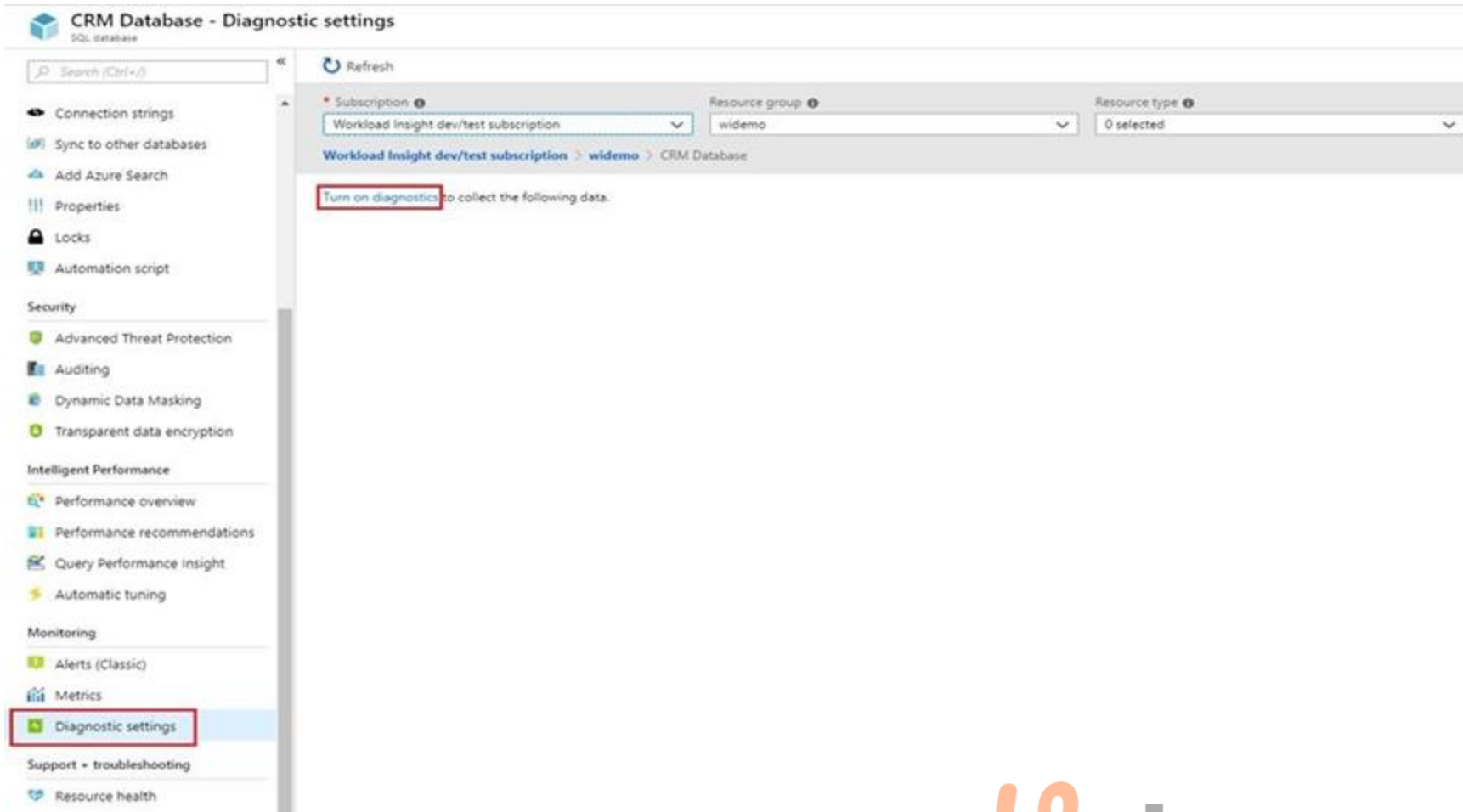
Section:

Explanation:

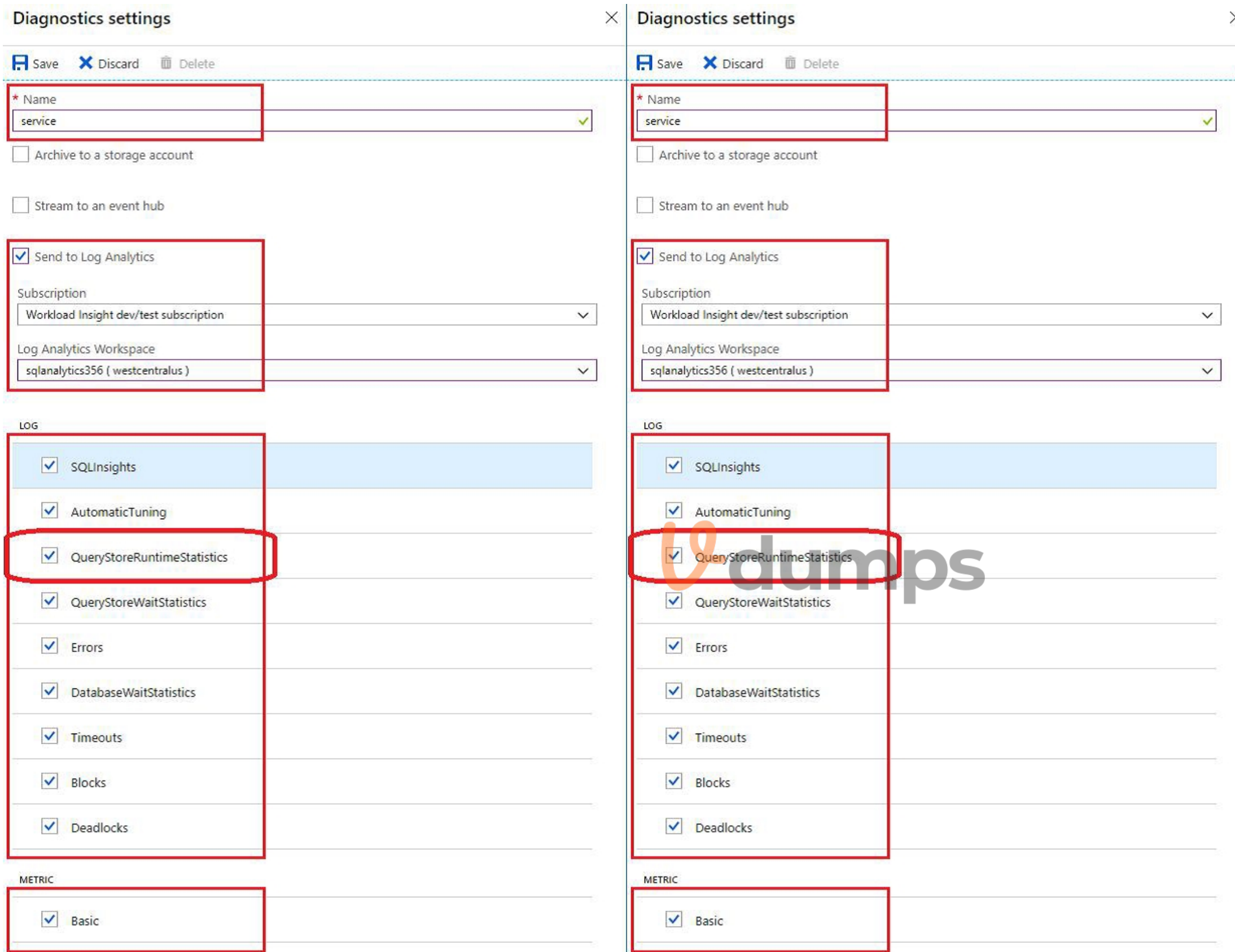
To enable streaming of diagnostic telemetry for a single or a pooled database, follow these steps:

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

Vdumps



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



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 12

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

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

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

NOTE: Each correct selection is worth one point.

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

Correct Answer: A, B

Section:

Explanation:

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

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

Reference:

<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>

QUESTION 13

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

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

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

Correct Answer: B

Section:

Explanation:

There are three types of Application Insights availability tests:

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

Multi-step web test

Custom Track Availability Tests

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

You can set up availability tests for any HTTP or HTTPS endpoint that is accessible from the public internet. You don't have to make any changes to the website you're testing. In fact, it doesn't even have to be a site you own.

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

Reference:

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

QUESTION 14

You have a multi-tier application. The front end of the application is hosted in Azure App Service. You need to identify the average load times of the application pages.

What should you use?

- A. Azure Application Insights

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

Correct Answer: A

Section:

Explanation:

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

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

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

Reference:

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

QUESTION 15

SIMULATION

You need to create an instance of Azure Application Insights named az400-9940427-main and configure the instance to receive telemetry data from an Azure web app named az400-9940427-main.

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

- A. See solution below.

Correct Answer: A

Section:

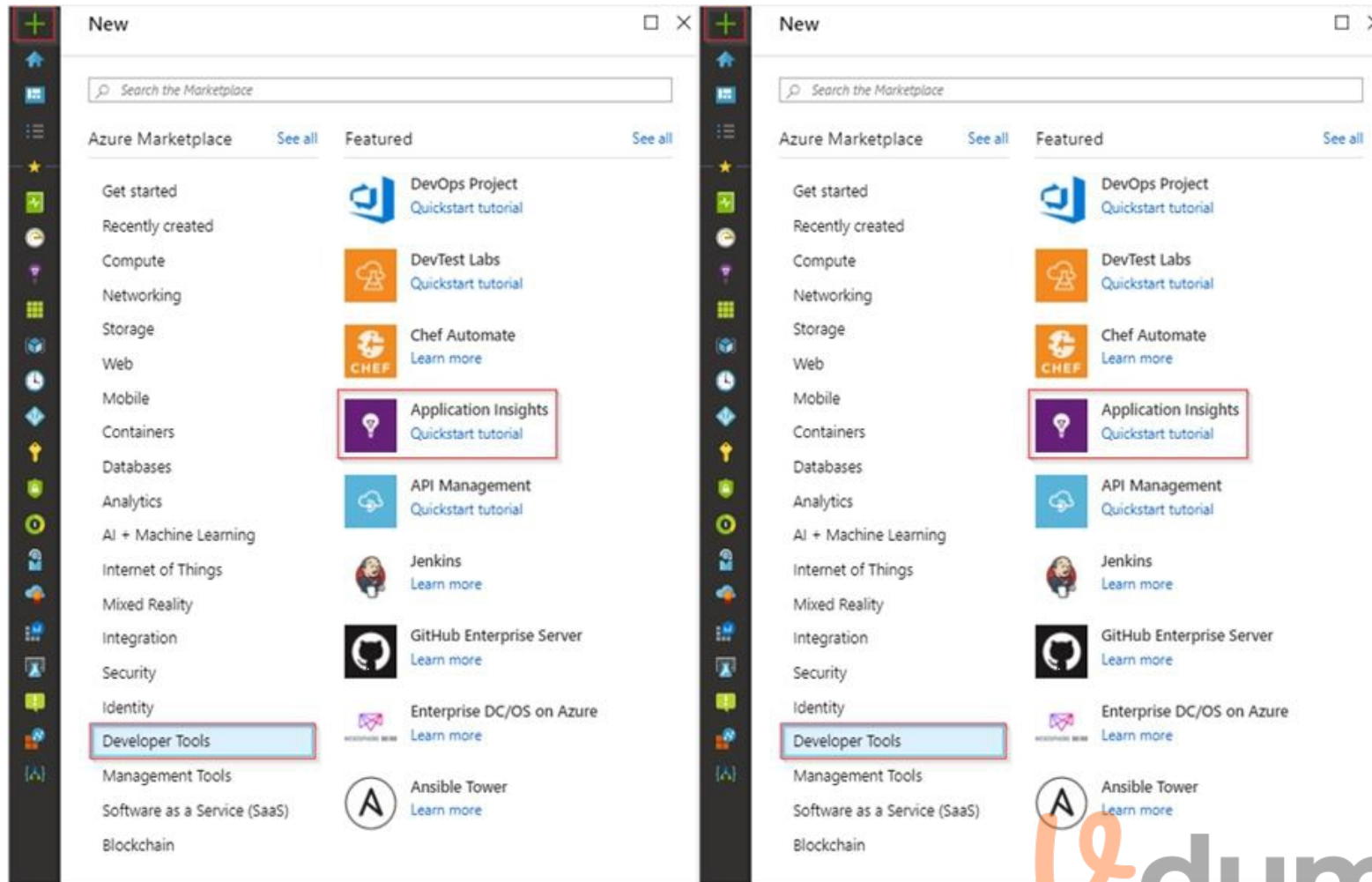
Explanation:

Step 1: Create an instance of Azure Application Insights

1. Open Microsoft Azure Portal

2. Log into your Azure account, Select Create a resource > Developer tools > Application Insights.



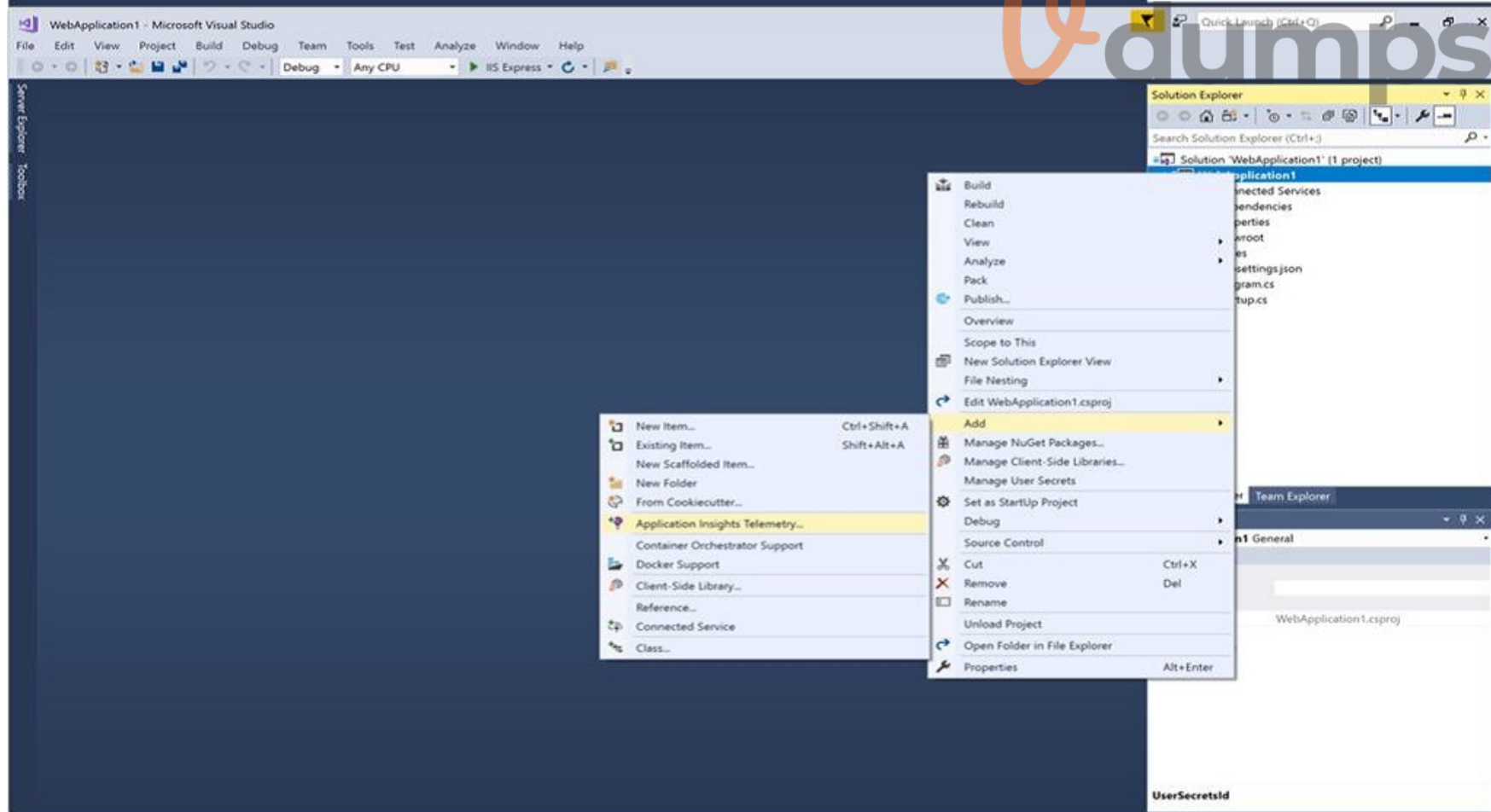
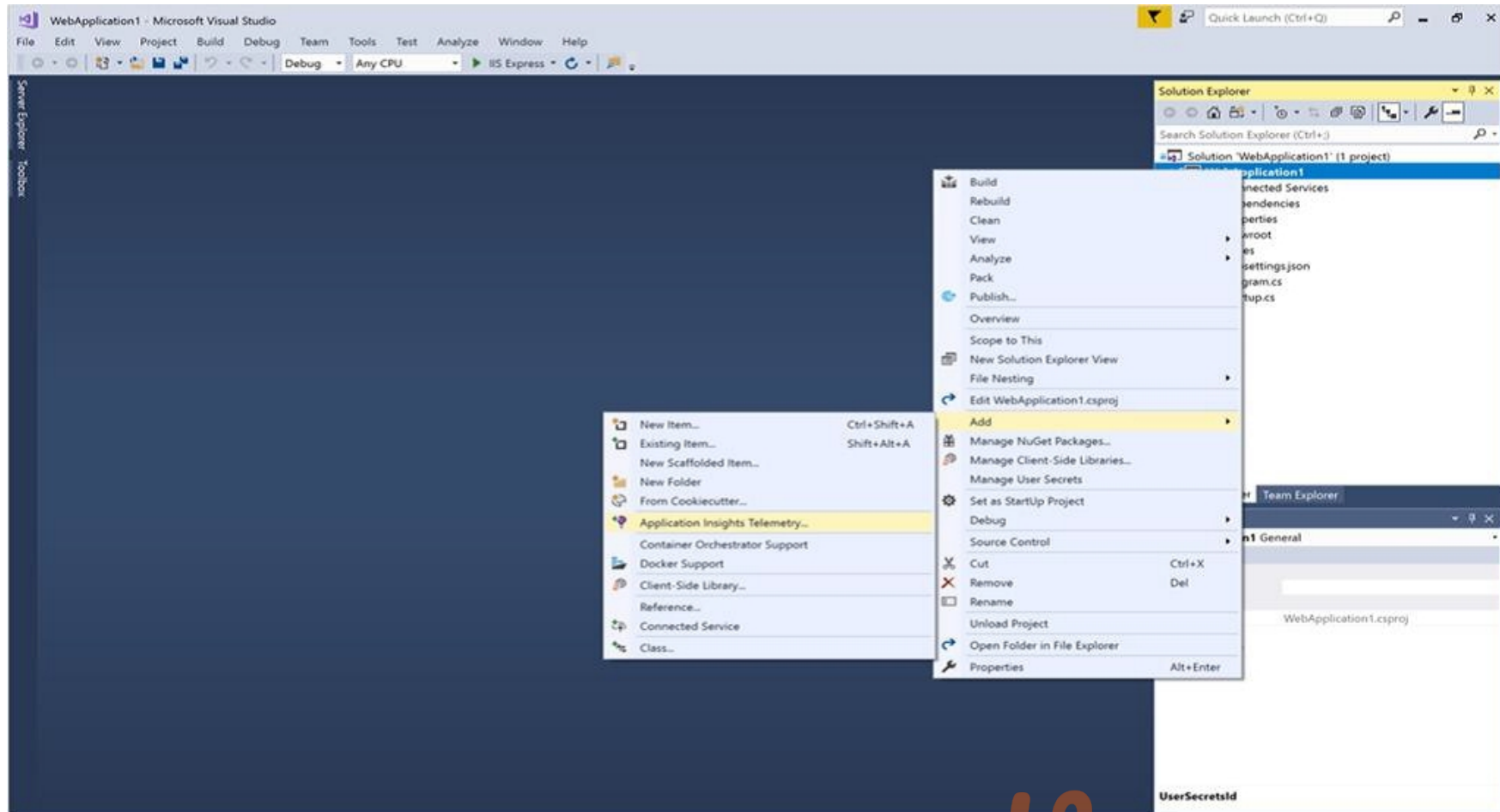


3. Enter the following settings, and then select Review + create.

Name: az400-9940427-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 16

HOTSPOT

You have a project in Azure DevOps named Contoso App that contains pipelines in Azure Pipelines for GitHub repositories.

You need to ensure that developers receive Microsoft Teams notifications when there are failures in a pipeline of Contoso App.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

@azure pipelines	<input type="text"/>	<input type="text"/>
	feedback	https://dev.azure.com/contoso/contoso-app/
	signin	https://dev.azure.com/contoso/contoso-app/_build
	subscribe	https://dev.azure.com/contoso/contoso-app/_packaging
	subscriptions	https://dev.azure.com/contoso/contoso-app/_work-items

 dumps

Answer Area:

Answer Area

@azure pipelines	<input type="text"/>	<input type="text"/>
	feedback	https://dev.azure.com/contoso/contoso-app/
	signin	https://dev.azure.com/contoso/contoso-app/_build
	subscribe	https://dev.azure.com/contoso/contoso-app/_packaging
	subscriptions	https://dev.azure.com/contoso/contoso-app/_work-items

Section:

Explanation:

Box 1: subscribe

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

@azure pipelines subscribe [project url]

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

Subscribe to a pipeline or all pipelines in a project to receive notifications:
@azure pipelines subscribe [pipeline url/ project url]

QUESTION 17

HOTSPOT

You use Azure DevOps to manage the build and deployment of an app named App1.

You have release pipeline that deploys a virtual machine named VM1.

You plan to monitor the release pipeline by using Azure Monitor.

You need to create an alert to monitor the performance of VM1. The alert must be triggered when the average CPU usage exceeds 70 percent for five minutes. The alert must calculate the average once every minute.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Aggregation granularity (Period): ▼
1 minute
5 minutes

Threshold value: ▼
Static
Dynamic

Operator: ▼
Greater than
Greater than or equal to
Less than or equal to
Less than



Answer Area:

Answer Area

Aggregation granularity (Period):

	▼
1 minute	
5 minutes	

Threshold value:

	▼
Static	
Dynamic	

Operator:

	▼
Greater than	
Greater than or equal to	
Less than or equal to	
Less than	

Section:

Explanation:

Box 1: 5 minutes

The alert must calculate the average once every minute.

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

Box 2: Static

Box 3: Greater than

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

Target resource: myAppServicePlan

Metric: Percentage CPU

Condition Type: Static

Dimensions

Instance = InstanceName1, InstanceName2

Time Aggregation: Average

Period: Over the last 5 mins

Frequency: 1 min

Operator: GreaterThan

Threshold: 70

Like before, this rule monitors if the average CPU usage for the last 5 minutes exceeds 70%.

Aggregation granularity

Reference:

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

QUESTION 18

Your company uses ServiceNow for incident management.

You develop an application that runs on Azure.

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

Which Azure Log Analytics solution should you use?

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

Correct Answer: C

Section:

Explanation:

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

ITSMC supports connections with the following ITSM tools:

ServiceNow

System Center Service Manager

Provance

Cherwell

With ITSMC, you can

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

Reference:

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

QUESTION 19

You use Azure SQL Database Intelligent Insights and Azure Application Insights for monitoring.

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

Which query language should you use?

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



Correct Answer: A

Section:

Explanation:

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

Reference:

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

QUESTION 20

Your company creates a web application.

You need to recommend a solution that automatically sends to Microsoft Teams a daily summary of the exceptions that occur in the application. Which two Azure services should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

E. Azure Application Insights

Correct Answer: A, E

Section:

Explanation:

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

Note: Periodical reports help keep a team informed on how their business critical services are doing. Developers, DevOps/SRE teams, and their managers can be productive with automated reports reliably delivering insights without requiring everyone to sign in the portal. Such reports can also help identify gradual increases in latencies, load or failure rates that may not trigger any alert rules.

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

Automate reports with Microsoft Flow

Automate reports with Logic Apps

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/asp-net-exceptions>

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/automate-custom-reports>

QUESTION 21

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

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

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

Collect crash reports for issue analysis.

Distribute beta releases to your testers.

Get user feedback on the functionality of new apps.

What should you include in the recommendation?

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

Correct Answer: A

Section:

Explanation:

The "Exploratory Testing" extension is now "Test & Feedback" and is now Generally Available.

Anyone can now test web apps and give feedback, all directly from the browser on any platform: Windows, Mac, or Linux. Available for Google Chrome and Mozilla Firefox (required version 50.0 or above) currently. Support for Microsoft Edge is in the pipeline and will be enabled once Edge moves to a Chromium-compatible web platform.

Reference:

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

QUESTION 22

You are monitoring the health and performance of an Azure web app by using Azure Application Insights. You need to ensure that an alert is sent when the web app has a sudden rise in performance issues and failures. What should you use?

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



Correct Answer: D

Section:

Explanation:

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

Reference:

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

QUESTION 23

You have a private GitHub repository.

You need to display the commit status of the repository on Azure Boards.

What should you do first?

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

Correct Answer: C

Section:

Explanation:

To connect Azure Boards to GitHub.com, connect and configure from Azure Boards. Or, alternatively, install and configure the Azure Boards app from GitHub. Both methods have been streamlined and support authenticating and operating via the app rather than an individual.

Note (see step 4 below):

Add a GitHub connection:

1. Sign into Azure Boards.
2. Choose (1) Project Settings, choose (2) GitHub connections and then (3) Connect your GitHub account.
3. If this is your first time connecting to GitHub from Azure Boards, you will be asked to sign in using your GitHub credentials. Choose an account for which you are an administrator for the repositories you want to connect to.
4. The Add GitHub Repositories dialog automatically displays and selects all GitHub.com repositories for which you are an administrator. Unselect any repositories that you don't want to participate in the integration.



Add GitHub repositories

Add the GitHub repositories you want to use with your Azure Boards.

Filter by keywords

Viewing 4, 4 selected

- JamalHart/fabrikam- apps-2
- JamalHart/fabrikam- demo
- JamalHart/fabrikam- open- source
- JamalHart/fabrikam- suite

Save

Reference:

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

QUESTION 24

You are integrating Azure Pipelines and Microsoft Teams.

You install the Azure Pipelines app in Microsoft Teams.

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

You subscribe to Project1 in Microsoft Teams.

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

What should you do first?

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

Correct Answer: A

Section:

Explanation:

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

```
@azure pipelines subscribe [project url]
```

The project URL can be to any page within your project (except URLs to pipelines).

For example:

```
@azure pipelines subscribe https://dev.azure.com/myorg/myproject/
```

Reference:

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

QUESTION 25

The logo for Vdumps.com, featuring a stylized orange 'V' followed by the word 'dumps' in a grey, lowercase, sans-serif font.

You have an Azure DevOps organization named Contoso.
You need to receive Microsoft Teams notifications when work items are updated.
What should you do?

- A. From Azure DevOps, configure a service hook subscription
- B. From Microsoft Teams, configure a connector
- C. From Microsoft Teams admin center, configure external access
- D. From Microsoft Teams, add a channel
- E. From Azure DevOps, install an extension

Correct Answer: A

Section:

Explanation:

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>

QUESTION 26

DRAG DROP

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

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

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



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

NOTE: Each correct selection is worth one point.

Select and Place:

Values**Answer Area**`count ()``Event``makelist (EventID)``| where TimeGenerated > ago(12h)``makeset (EventID)``| order by TimeGenerated desc``mv-expand``| [] [] by Computer``project``render``summarize`**Correct Answer:****Values****Answer Area**`count ()``Event``[]``| where TimeGenerated > ago(12h)``makeset (EventID)``| order by TimeGenerated desc``mv-expand``| [summarize] [makelist (EventID)] by Computer``project``render``[]`**Section:****Explanation:**

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 27

HOTSPOT

You have an Azure web app named Webapp1.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

exceptions
pageViews
requests
traces

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

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

Answer Area:

Answer Area

exceptions
pageViews
requests
traces

```
| where
```

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

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

vdumps

Section:

Explanation:

Box 1: requests

Failed requests (requests/failed):

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

Kusto code:

```
requests
```

```
| where success == 'False'
```

Box 2: success == false

Reference:

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

02 - Develop an instrumentation strategy

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overview

Woodgrove Bank is a financial services company that has a main office in the United Kingdom.

Technical Requirements and Planned Changes

Planned Changes

Woodgrove Bank plans to implement the following project management changes:

Implement Azure DevOps for project tracking.

Centralize source code control in private GitHub repositories.

Implement Azure Pipelines for build pipelines and release pipelines.

Woodgrove Bank plans to implement the following changes to the identity environment:

Deploy an Azure AD tenant named woodgrovebank.com.

Sync the Active Directory domain to Azure AD.

Configure App1 to use a service principal.

Integrate GitHub with Azure AD.

Woodgrove Bank plans to implement the following changes to the core apps:

Migrate App1 to ASP.NET Core.

Integrate Azure Pipelines and the third-party build tool used to develop App2.

Woodgrove Bank plans to implement the following changes to the DevOps environment:

Deploy App1 to Azure App Service.

Implement source control for the DB1 schema.

Migrate all the source code from TFS1 to GitHub.

Deploy App2 to an Azure virtual machine named VM1.

Merge the POC branch into the GitHub default branch.

Implement an Azure DevOps dashboard for stakeholders to monitor development progress.

Technical Requirements

Woodgrove Bank identifies the following technical requirements:

The initial databases for new environments must contain both schema and reference data.

An Azure Monitor alert for VM1 must be configured to meet the following requirements:

- Be triggered when average CPU usage exceeds 80 percent for 15 minutes.

- Calculate CPU usage averages once every minute.

- The commit history of the POC branch must replace the history of the default branch.

The commit history of the POC branch must replace the history of the default branch.

The Azure DevOps dashboard must display the metrics shown in the following table.

Number	Required data
1	A comparison between the work the development team planned to deliver and what was delivered
2	The status of the environments in a release definition
3	The total number of results from a work item query

Access to Azure DevOps must be restricted to specific IP addresses.

Page load times for App1 must be captured and monitored.

Administrative effort must be minimized.



QUESTION 1

HOTSPOT

You need to configure the alert for VM1. The solution must meet the technical requirements.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Alert logic

Threshold ⓘ

Static Dynamic

Operator ⓘ

Greater than ▼

Aggregation type * ⓘ

Average ▼

Threshold value * ⓘ

▼

%

Condition preview

Whenever the average percentage cpu is greater than <logic undefined> %

Evaluated based on

Aggregation granularity (Period) * ⓘ

5 minutes ▼

Frequency of evaluation ⓘ

Every 1 Minute ▼

Answer Area:

Alert logic

Threshold ⓘ

Static Dynamic

Operator ⓘ

Greater than ▾

Aggregation type * ⓘ

Average ▾

Threshold value * ⓘ

▾ %

Condition preview

Whenever the average percentage cpu is greater than <logic undefined> %

Evaluated based on

Aggregation granularity (Period) * ⓘ

5 minutes ▾

Frequency of evaluation ⓘ

Every 1 Minute ▾

Section:

Explanation:

Setting 1: Threshold value

Set to 80 %

Scenario: An Azure Monitor alert for VM1 must be configured to meet the following requirements:

Be triggered when average CPU usage exceeds 80 percent for 15 minutes.

Calculate CPU usage averages once every minute.

Setting 2: Aggregation granularity

Set to 15 minutes.

01 - Develop a Site Reliability Engineering (SRE) strategy

QUESTION 1

You have a build pipeline in Azure Pipelines that occasionally fails.

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

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

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

NOTE: Each correct selection is worth one point.

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

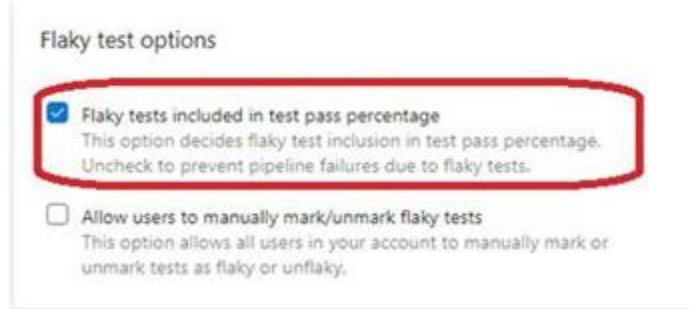
Correct Answer: B, D



Section:

Explanation:

D: You can mark or unmark a test as flaky based on analysis or context, by choosing Flaky.
To configure flaky test management, choose Project settings, and select Test management in the Pipelines section.
B:
Slide the On/Off button to On.



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

QUESTION 2

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



Correct Answer: C

Section:

Explanation:

Scenarios and use cases for gates include:

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

Quality validation. Query metrics from tests on the build artifacts such as pass rate or code coverage and deploy only if they are within required thresholds.
Use Quality Gates to integrate monitoring into your pre-deployment or post-deployment. This ensures that you are meeting the key health/performance metrics (KPIs) as your applications move from dev to production and any differences in the infrastructure environment or scale is not negatively impacting your KPIs.
Note: Gates allow automatic collection of health signals from external services, and then promote the release when all the signals are successful at the same time or stop the deployment on timeout. Typically, gates are used in connection with incident management, problem management, change management, monitoring, and external approval systems.

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

QUESTION 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 process to the correct customers. Each work item process may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Processes

- Agile
- CMMI
- Scrum
- XP

Answer Area

- Litware
- Contoso:
- A. Datum:



Correct Answer:

Processes

-
-
-
- XP

Answer Area

- Litware
- Contoso:
- A. Datum:

- Scrum
- Agile
- CMMI

Section:

Explanation:

Box 1: Scrum

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

Box 2: Agile

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

Box 3: CMMI

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

Incorrect Answers:

XP:

The work tracking objects contained within the default DevOps processes and DevOps process templates are Basic, Agile, CMMI, and Scrum XP (Extreme Programming) and DevOps are different things. They don't contradict with each other, they can be used together, but they have different base concepts inside them.

References:

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

QUESTION 4

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
 ✓

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

Test type:
 ▼

* URL ⓘ
 ✓

Parse dependent requests ⓘ

Enable retries for availability test failures: ⓘ

Test frequency ⓘ
 ▼

▼ Test locations
 4 location(s) configured

^ Success criteria

Test Timeout ⓘ
 ▼

HTTP response ⓘ

Status code must equal:

Content match ⓘ

Content must contain:

▼ Alerts
 Enabled



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

Hot Area:

Answer Area

The test will execute [answer choice].

	▼
every 30 seconds at a random location	
every 30 seconds per location	
every five minutes at a random location	
every five minutes per location	

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

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

Answer Area:

Answer Area



The test will execute [answer choice].

	▼
every 30 seconds at a random location	
every 30 seconds per location	
every five minutes at a random location	
every five minutes per location	

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

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

Section:

Explanation:

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 5

DRAG DROP

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

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

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

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

Select and Place:

Actions

Answer Area

Select the Recurrence trigger.

Create an Azure event hub.

Create an Azure logic app.

Select the HTTP request trigger.

Update the action group in Azure Monitor.

Select the Sliding Window trigger.



Correct Answer:

Actions

Answer Area

Select the Recurrence trigger.		Create an Azure logic app.
Create an Azure event hub.		Select the HTTP request trigger.
	⬅	Update the action group in Azure Monitor.
	➡	
Select the Sliding Window trigger.		



Section:

Explanation:

Box 1: Create an Azure logic app.

Box 2: Select the HTTP request trigger.

Box 3: Updated the action group in Azure Monitor.

Reference:

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

QUESTION 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 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

Correct Answer: B

Section:

Explanation:

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

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

Reference:

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

QUESTION 7

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

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

You have an 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

Correct Answer: B

Section:



QUESTION 8

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

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

Correct Answer: B

Section:

Explanation:

Instead implement Continuous Assurance for the project.

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

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

QUESTION 9

Your company uses the following resources:

Windows Server 2019 container images hosted in an Azure Container Registry.

Azure virtual machines that run the latest version of Ubuntu

An Azure Log Analytics workspace

Azure Active Directory (Azure AD)

An Azure key vault

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

NOTE: Each correct selection is worth one point.

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

Correct Answer: C, E

Section:

Explanation:

QUESTION 10

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.



Correct Answer: B

Section:

Explanation:

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

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

Reference:

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

QUESTION 11

You configure an Azure Application Insights availability test.

You need to notify the customer services department at your company by email when availability is degraded. You create an Azure logic app that will handle the email and follow up actions.

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

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

Correct Answer: A

Section:

Explanation:

You can use webhooks to route an Azure alert notification to other systems for post-processing or custom actions. You can use a webhook on an alert to route it to services that send SMS messages, to log bugs, to notify a team via chat or messaging services, or for various other actions.

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

QUESTION 12

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

You use Azure DevOps to build a containerized app named App1 and deploy App1 to an Azure container instance named ACI1. You need to restart ACI1 when App1 stops responding.

What should you do?

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

Correct Answer: B

Section:

Explanation:

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



QUESTION 13

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

Correct Answer: D

Section:

Explanation:

Azure Platform as a Service (PaaS) resources, like Azure SQL and Web Sites (Web Apps), can emit performance metrics data natively to Log Analytics. The Premium plan will retain up to 12 months of data, giving you an excellent baseline ability.

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

B: Intelligent Insights analyzes database performance by comparing the database workload from the last hour with the past seven-day baseline workload. However, we need handle application metrics as well.

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

QUESTION 14

You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 that is configured for autoscaling. You use Azure DevOps to build a web app named App1 and deploy App1 to VMSS1. App1 is used heavily and has usage patterns that vary on a weekly basis. You need to recommend a solution to detect an abnormal rise in the rate of failed requests to App1. The solution must minimize administrative effort. What should you include in the recommendation?

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

Correct Answer: A

Section:

Explanation:

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

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

QUESTION 15

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.

- A. See solution below.

Correct Answer: A

Section:

Explanation:

Enable Remote Debugging

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

1. Navigate in the Azure portal to your function app fa-11566895
2. Go to the "Application settings"
3. Under "Debugging" set Remote Debugging to On and set Remote Visual Studio version to 2017.

Reference:

<https://www.locktar.nl/uncategorized/azure-remote-debugging-manually-in-visual-studio-2017/>



QUESTION 16

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.

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

Correct Answer: C

Section:**Explanation:**

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

Kusto uses a role-based access control (RBAC) model, under which authenticated principals are mapped to roles, and get access according to the roles they're assigned. Note: Azure Data Explorer is a highly scalable and secure analytics service that enables you to do rich exploration of structured and unstructured data for instant insights. Optimized for ad-hoc queries, Azure Data Explorer enables rich data exploration over raw, structured, and semi-structured data delivering fast time to insight. Query with a modern, intuitive query language that offers fast, ad-hoc, and advanced query capabilities over high-rate data volumes and varieties

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

QUESTION 17

You are automating the testing process for your company.

You need to automate UI testing of a web application.

Which framework should you use?

- A. JaCoco
- B. Playwright
- C. Xamarin.UITest
- D. Microsoft.CodeAnalysis

Correct Answer: B

Section:**Explanation:**

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

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

QUESTION 18

You are building an ASP.NET Core application.

You plan to create an application utilization baseline by capturing telemetry data.

You need to add code to the application to capture the telemetry data. The solution must minimize the costs of storing the telemetry data. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point

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

Correct Answer: B, D

Section:**Explanation:**

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>

QUESTION 19

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

Correct Answer: D

Section:

Explanation:

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

Reference:

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

QUESTION 20

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

Correct Answer: B

Section:

Explanation:

Instead implement Continuous Assurance for the project.

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

QUESTION 21

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

Correct Answer: B

Section:

Explanation:

Instead implement Continuous Assurance for the project.

Reference:

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

QUESTION 22

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

Correct Answer: A

Section:

Explanation:

The basic idea behind Continuous Assurance (CA) is to setup the ability to check for "drift" from what is considered a secure snapshot of a system. Support for Continuous Assurance lets us treat security truly as a 'state' as opposed to a 'point in time' achievement. This is particularly important in today's context when 'continuous change' has become a norm. There can be two types of drift:

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

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

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

QUESTION 23

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

Correct Answer: A

Section:

Explanation:

QUESTION 24

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

What should you configure?

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

Correct Answer: C

Section:

Explanation:

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

Incorrect Answers:

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

Reference:

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



QUESTION 25

You are designing a strategy to monitor the baseline metrics of Azure virtual machines that run Windows Server. You need to collect detailed data about the processes running in the guest operating system.

Which two agents should you deploy? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Correct Answer: B, D

Section:

Explanation:

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

	Azure Monitor agent (preview)	Diagnostics extension (WAD)	Log Analytics agent	Dependency agent
Environments supported	Azure	Azure	Azure Other cloud On-premises	Azure Other cloud On-premises
Agent requirements	None	None	None	Requires Log Analytics agent
Data collected	Event Logs Performance	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>

QUESTION 26

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

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

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

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

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

Solution: From Azure Monitor, create an action group.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

Explanation:

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

triggered.

Reference:

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

02 - Develop a Site Reliability Engineering (SRE) strategy

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

Litware, Inc. is an independent software vendor (ISV). Litware has a main office and five branch offices.

Existing Environment

Application Architecture

The company's primary application is a single monolithic retirement fund management system based on ASP.NET web forms that use logic written in VB.NET. Some new sections of the application are written in C#.

Variations of the application are created for individual customers. Currently, there are more than 80 live code branches in the application's code base.

The application was developed by using Microsoft Visual Studio. Source code is stored in Team Foundation Server (TFS) in the main office. The branch offices access the source code by using TFS proxy servers.

Architectural Issues

Litware focuses on writing new code for customers. No resources are provided to refactor or remove existing code. Changes to the code base take a long time, as dependencies are not obvious to individual developers.

Merge operations of the code often take months and involve many developers. Code merging frequently introduces bugs that are difficult to locate and resolve.

Customers report that ownership costs of the retirement fund management system increase continually. The need to merge unrelated code makes even minor code changes expensive.

Customers report that bug reporting is overly complex.

Requirements

Planned Changes

Litware plans to develop a new suite of applications for investment planning. The investment planning applications will require only minor integration with the existing retirement fund management system.

The investment planning applications suite will include one multi-tier web application and two iOS mobile applications. One mobile application will be used by employees; the other will be used by customers.

Litware plans to move to a more agile development methodology. Shared code will be extracted into a series of packages.

Litware has started an internal cloud transformation process and plans to use cloud-based services whenever suitable.

Litware wants to become proactive in detecting failures, rather than always waiting for customer bug reports.

Technical Requirements

The company's investment planning applications suite must meet the following requirements:

New incoming connections through the firewall must be minimized.

Members of a group named Developers must be able to install packages.

The principle of least privilege must be used for all permission assignments.

A branching strategy that supports developing new functionality in isolation must be used.

Members of a group named Team Leaders must be able to create new packages and edit the permissions of package feeds. Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use. By default, all releases must remain available for 30 days, except for production releases, which must be kept for 60 days. Code quality and release quality are critical. During release, deployments must not proceed between stages if any active bugs are logged against the release. The mobile applications must be able to call the share pricing service of the existing retirement fund management system. Until the system is upgraded, the service will only support basic authentication over HTTPS. The required operating system configuration for the test servers changes weekly. Azure Automation State Configuration must be used to ensure that the operating system on each test server is configured the same way when the servers are created and checked periodically.

Current Technical Issue

The test servers are configured correctly when first deployed, but they experience configuration drift over time. Azure Automation State Configuration fails to correct the configurations.

Azure Automation State Configuration nodes are registered by using the following command.

```
Register-AzureRmAutomationDscNode
-ResourceGroupName 'TestResourceGroup'
-AutomationAccountName 'LitwareAutomationAccount'
-AzureVMName $vmname
-ConfigurationMode 'ApplyOnly'
```

QUESTION 1

HOTSPOT

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Application Architecture

The company's primary application is a single monolithic retirement fund management system based on ASP.NET web forms that use logic written in VB.NET. Some new sections of the application are written in C#.

Variations of the application are created for individual customers. Currently, there are more than 80 live code branches in the application's code base.

The application was developed by using Microsoft Visual Studio. Source code is stored in Team Foundation Server (TFS) in the main office. The branch offices access the source code by using TFS proxy servers.

Architectural Issues

Litware focuses on writing new code for customers. No resources are provided to refactor or remove existing code. Changes to the code base take a long time, as dependencies are not obvious to individual developers.

Merge operations of the code often take months and involve many developers. Code merging frequently introduces bugs that are difficult to locate and resolve. Customers report that ownership costs of the retirement fund management system increase continually. The need to merge unrelated code makes even minor code changes expensive.

Customers report that bug reporting is overly complex.

Planned changes

Litware plans to develop a new suite of applications for investment planning. The investment planning applications will require only minor integration with the existing retirement fund management system.

The investment planning applications suite will include one multi-tier web application and two iOS mobile application. One mobile application will be used by employees; the other will be used by customers.

Litware plans to move to a more agile development methodology. Shared code will be extracted into a series of packages.

Litware has started an internal cloud transformation process and plans to use cloud-based services whenever suitable.

Litware wants to become proactive in detecting failures, rather than always waiting for customer bug reports.

Technical requirements

The company's investment planning applications suite must meet the following requirements:

New incoming connections through the firewall must be minimized.

Members of a group named Developers must be able to install packages.

The principle of least privilege must be used for all permission assignments.

A branching strategy that supports developing new functionality in isolation must be used.

Members of a group named Team Leaders must be able to create new packages and edit the permissions of package feeds.

Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use.

By default, all releases must remain available for 30 days, except for production releases, which must be kept for 60 days.

Code quality and release quality are critical. During release, deployments must not proceed between stages if any active bugs are logged against the release.

The mobile applications must be able to call the share pricing service of the existing retirement fund management system. Until the system is upgraded, the service will only support basic authentication over HTTPS.

The required operating system configuration for the test servers changes weekly. Azure Automation State Configuration must be used to ensure that the operating system on each test server is configured the same way when the servers are created and checked periodically.

Current Technical Issue

The test servers are configured correctly when first deployed, but they experience configuration drift over time. Azure Automation State Configuration fails to correct the configurations.

Azure Automation State Configuration nodes are registered by using the following command.

```
Register-AzureRmAutomationDscNode  
-ResourceGroupName 'TestResourceGroup'  
-AutomationAccountName 'LitwareAutomationAccount'  
-AzureVMName $vmname  
-ConfigurationMode 'ApplyOnly'
```

How should you complete the code to initialize App Center in the mobile application? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

[MSAnalytics.self, [MSDistribute.self, [MSPush.self,	MSAnalytics.self] MSCrashes.self] MSDistribute.self]

Answer Area:

Answer Area

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

[MSAnalytics.self, [MSDistribute.self, [MSPush.self,	MSAnalytics.self] MSCrashes.self] MSDistribute.self]

Section:

Explanation:

Scenario: Visual Studio App Center must be used to centralize the reporting of mobile application crashes and device types in use. In order to use App Center, you need to opt in to the service(s) that you want to use, meaning by default no services are started and you will have to explicitly call each of them when starting the SDK. Insert the following line to start the SDK in your app's AppDelegate class in the didFinishLaunchingWithOptions method. `MSAppCenter.start("{Your App Secret}", withServices: [MSAnalytics.self, MSCrashes.self])` References: <https://docs.microsoft.com/en-us/appcenter/sdk/getting-started/ios>

03 - Develop a Site Reliability Engineering (SRE) strategy

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a manufacturing company that has a main office in Chicago.

Existing Environment

Contoso plans to improve its IT development and operations processes by implementing Azure DevOps principles. Contoso has an Azure subscription and creates an Azure DevOps organization.

The Azure DevOps organization includes:

The Docker extension

A deployment pool named Pool7 that contains 10 Azure virtual machines that run Windows Server 2019

The Azure subscription contains an Azure Automation account.

Requirements

Planned changes

Contoso plans to create projects in Azure DevOps as shown in the following table.



Project name	Project details
Project 1	Project1 will provide support for incremental builds and third-party SDK components
Project 2	Project2 will use an automatic build policy. A small team of developers named Team2 will work independently on changes to the project. The Team2 members will not have permissions to Project2.
Project 3	Project3 will be integrated with SonarQube
Project 4	Project4 will provide support for a build pipeline that creates a Docker image and pushes the image to the Azure Container Registry. Project4 will use an existing Dockerfile.
Project 5	Project5 will contain a Git repository in Azure Repos and a continuous integration trigger that will initiate a build in response to any change except for changes within /folder1 of the repository.
Project 6	Project6 will provide support for build and deployment pipelines. Deployment will be allowed only if the number of current work items representing active software bugs is 0.
Project 7	Project7 will contain a target deployment group named Group7 that maps to Pool7. Project7 will use Azure Automation State Configuration to maintain the desired state of the computers in Group7.

Technical requirements

Contoso identifies the following technical requirements:

Implement build agents for Project1.

Whenever possible, use Azure resources.

Avoid using deprecated technologies.

Implement a code flow strategy for Project2 that will:

- Enable Team2 to submit pull requests for Project2.
- Enable Team2 to work independently on changes to a copy of Project2.

- Ensure that any intermediary changes performed by Team2 on a copy of Project2 will be subject to the same restrictions as the ones defined in the build policy of Project2. Whenever possible, implement automation and minimize administrative effort.

Implement Project3, Project5, Project6, and Project7 based on the planned changes.

Implement Project4 and configure the project to push Docker images to Azure Container Registry.

QUESTION 1

You add the virtual machines as managed nodes in Azure Automation State Configuration.

You need to configure the managed computers in Pool7.

What should you do next?

- A. Modify the RefreshMode property of the Local Configuration Manager (LCM).
- B. Run the Register-AzureRmAutomationDscNode Azure Powershell cmdlet.
- C. Modify the ConfigurationMode property of the Local Configuration Manager (LCM).
- D. Install PowerShell Core.

Correct Answer: B

Section:

Explanation:

The Register-AzureRmAutomationDscNode cmdlet registers an Azure virtual machine as an APS Desired State Configuration (DSC) node in an Azure Automation account.

Scenario: The Azure DevOps organization includes:

The Docker extension

A deployment pool named Pool7 that contains 10 Azure virtual machines that run Windows Server 2019

Project 7	Project7 will contain a target deployment group named Group7 that maps to Pool7. Project7 will use Azure Automation State Configuration to maintain the desired state of the computers in Group7.
-----------	---

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azurermsautomation/register-azurermsautomationdscnode>



QUESTION 2

DRAG DROP

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Background

Contoso, Ltd. is a manufacturing company that has a main office in Chicago.

Contoso plans to improve its IT development and operations processes by implementing Azure DevOps principles. Contoso has an Azure subscription and creates an Azure DevOps organization.

The Azure DevOps organization includes:

The Docker extension

A deployment pool named Pool7 that contains 10 Azure virtual machines that run Windows Server 2019

The Azure subscription contains an Azure Automation account.

Contoso plans to create projects in Azure DevOps as shown in the following table.

Project name	Project details
Project 1	Project1 will provide support for incremental builds and third-party SDK components
Project 2	Project2 will use an automatic build policy. A small team of developers named Team2 will work independently on changes to the project. The Team2 members will not have permissions to Project2.
Project 3	Project3 will be integrated with SonarQube
Project 4	Project4 will provide support for a build pipeline that creates a Docker image and pushes the image to the Azure Container Registry. Project4 will use an existing Dockerfile.
Project 5	Project5 will contain a Git repository in Azure Reports and a continuous integration trigger that will initiate a build in response to any change except for changes within /folder1 of the repository.
Project 6	Project6 will provide support for build and deployment pipelines. Deployment will be allowed only if the number of current work items representing active software bugs is 0.
Project 7	Project7 will contain a target deployment group named Group7 that maps to Pool7. Project7 will use Azure Automation State Configuration to maintain the desired state of the computers in Group7.

Technical requirements

Contoso identifies the following technical requirements:

Implement build agents for Project1.

Whenever possible, use Azure resources.

Avoid using deprecated technologies.

Implement a code flow strategy for Project2 that will:

-Enable Team2 to submit pull requests for Project2.

-Enable Team2 to work independently on changes to a copy of Project2.

-Ensure that any intermediary changes performed by Team2 on a copy of Project2 will be subject to the same restrictions as the ones defined in the build policy of Project2. Whenever possible implement automation and minimize administrative effort.

Implement Project3, Project5, Project6, and Project7 based on the planned changes

Implement Project4 and configure the project to push Docker images to Azure Container Registry.

You need to implement the code flow strategy for Project2 in Azure DevOps.

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

Select and Place:

Actions

Answer Area

Create a fork

Create a branch

Add a build policy for the fork

Add a build policy for the master branch

Create a repository

Add an application access policy.



Correct Answer:

Actions

Answer Area

Section:

Explanation:

Step 1: Create a repository

A Get repository, or repo, is a folder that you've told Git to help you track file changes in. You can have any number of repos on your computer, each stored in their own folder.

Step 2: Create a fork

Step 3: Add a build policy for the fork

Build policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.

Scenario:

Implement a code flow strategy for Project2 that will:

Enable Team2 to submit pull requests for Project2.

Enable Team2 to work independently on changes to a copy of Project2.

Ensure that any intermediary changes performed by Team2 on a copy of Project2 will be subject to the same restrictions as the ones defined in the build policy of Project2.

Project2 will use an automatic build policy. A small team of developers named Team2 will work independently on changes to the project. The Team2 members will not have permissions to Project2.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/repos/git/manage-your-branches>

QUESTION 3

DRAG DROP

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Background

Contoso, Ltd. is a manufacturing company that has a main office in Chicago.

Contoso plans to improve its IT development and operations processes by implementing Azure DevOps principles. Contoso has an Azure subscription and creates an Azure DevOps organization.

The Azure DevOps organization includes:

The Docker extension

A deployment pool named Pool7 that contains 10 Azure virtual machines that run Windows Server 2019

The Azure subscription contains an Azure Automation account.

Contoso plans to create projects in Azure DevOps as shown in the following table.

Project name	Project details
Project 1	Project1 will provide support for incremental builds and third-party SDK components
Project 2	Project2 will use an automatic build policy. A small team of developers named Team2 will work independently on changes to the project. The Team2 members will not have permissions to Project2.
Project 3	Project3 will be integrated with SonarQube
Project 4	Project4 will provide support for a build pipeline that creates a Docker image and pushes the image to the Azure Container Registry. Project4 will use an existing Dockerfile.
Project 5	Project5 will contain a Git repository in Azure Reports and a continuous integration trigger that will initiate a build in response to any change except for changes within /folder1 of the repository.
Project 6	Project6 will provide support for build and deployment pipelines. Deployment will be allowed only if the number of current work items representing active software bugs is 0.
Project 7	Project7 will contain a target deployment group named Group7 that maps to Pool7. Project7 will use Azure Automation State Configuration to maintain the desired state of the computers in Group7.

Technical requirements

Contoso identifies the following technical requirements:

Implement build agents for Project1.

Whenever possible, use Azure resources.

Avoid using deprecated technologies.

Implement a code flow strategy for Project2 that will:

-Enable Team2 to submit pull requests for Project2.

-Enable Team2 to work independently on changes to a copy of Project2.

-Ensure that any intermediary changes performed by Team2 on a copy of Project2 will be subject to the same restrictions as the ones defined in the build policy of Project2. Whenever possible implement automation and minimize administrative effort.

Implement Project3, Project5, Project6, and Project7 based on the planned changes

Implement Project4 and configure the project to push Docker images to Azure Container Registry.

You need to configure Azure Automation for the computers in Group7.

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

Select and Place:



Actions

Run the `Import-AzureRmAutomationDscConfiguration` Azure PowerShell cmdlet.

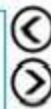
Create a Desired State Configuration (DSC) configuration file that has an extension of `.ps1`.

Run the `New-AzureRmResourceGroupDeployment` Azure PowerShell cmdlet.

Run the `Start-AzureRmAutomationDscCompilationJob` Azure PowerShell cmdlet.

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

Answer Area



Correct Answer:

Actions

Run the `New-AzureRmResourceGroupDeployment` Azure PowerShell cmdlet.

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

Answer Area

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

Run the `Import-AzureRmAutomationDscConfiguration` Azure PowerShell cmdlet.

Run the `Start-AzureRmAutomationDscCompilationJob` Azure PowerShell cmdlet.

Section:

Explanation:

Step 1: Create a Desired State Configuration (DSC) configuration file that has an extension of `.ps1`.

Step 2: Run the `Import-AzureRmAutomationDscConfiguration` Azure Powershell cmdlet

The `Import-AzureRmAutomationDscConfiguration` cmdlet imports an APS Desired State Configuration (DSC) configuration into Azure Automation. Specify the path of an APS script that contains a single DSC configuration.

Example:

```
PS C:\>Import-AzureRmAutomationDscConfiguration -AutomationAccountName "Contoso17"-ResourceGroupName "ResourceGroup01" -SourcePath "C:\DSC\client.ps1" -Force
```

This command imports the DSC configuration in the file named `client.ps1` into the Automation account named `Contoso17`. The command specifies the `Force` parameter. If there is an existing DSC configuration, this command replaces it.

Step 3: Run the Start-AzureRmAutomationDscCompilationJob Azure Powershell cmdlet

The Start-AzureRmAutomationDscCompilationJob cmdlet compiles an APS Desired State Configuration (DSC) configuration in Azure Automation.

References:

<https://docs.microsoft.com/en-us/powershell/module/azurermsautomation/import-azurermsautomationdscconfiguration>

<https://docs.microsoft.com/en-us/powershell/module/azurermsautomation/start-azurermsautomationdsc compilationjob>

01 - Develop a security and compliance plan

QUESTION 1

DRAG DROP

You are configuring an Azure DevOps deployment pipeline. The deployed application will authenticate to a web service by using a secret stored in an Azure key vault.

You need to use the secret in the deployment pipeline.

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

Select and Place:

Actions

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

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

Configure an access policy in the key vault.

Generate a self-signed certificate.

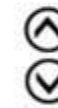
Add an Azure Resource Manager service connection to the pipeline.

Export a certificate from the key vault.

Answer Area



vdumps



Correct Answer:

Actions

-
- Add an app registration in Azure Active Directory (Azure AD).
-
- Generate a self-signed certificate.
-
- Export a certificate from the key vault.

Answer Area

- Create a service principal in Azure Active Directory (Azure AD)
- Configure an access policy in the key vault.
- Add an Azure Resource Manager service connection to the pipeline.



Section:

Explanation:

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

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

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

You need to secure access to your key vaults by allowing only authorized applications and users. To access the data from the vault, you will need to provide read (Get) permissions to the service principal that you will be using for authentication in the pipeline.

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



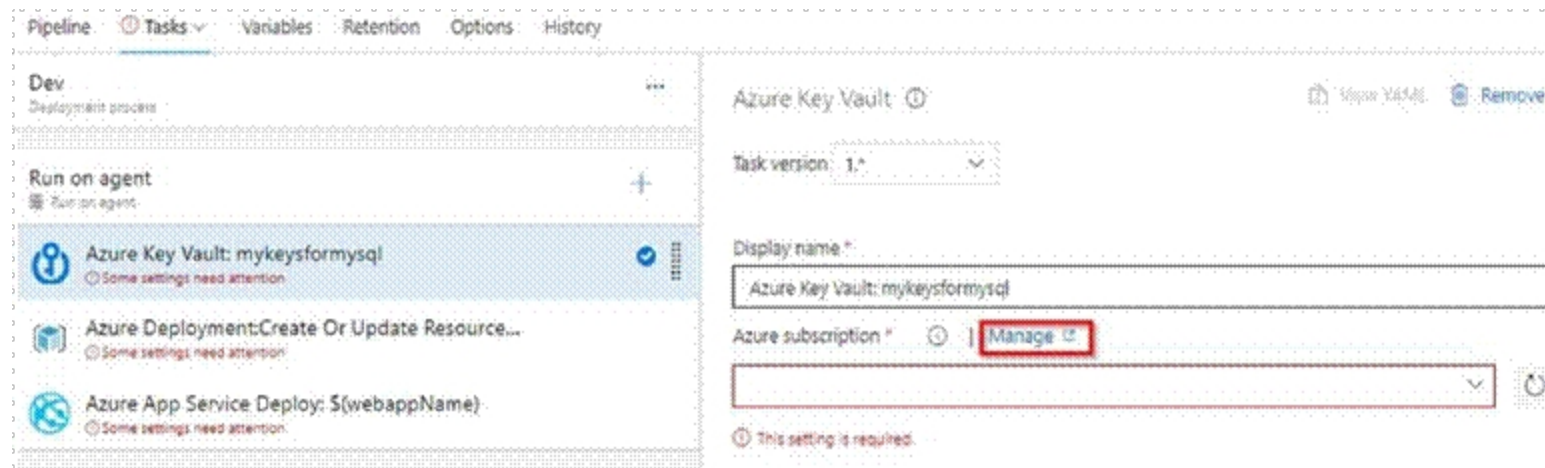
- Enable Access to:
- Azure Virtual Machines for deployment ⓘ
 - Azure Resource Manager for template deployment ⓘ
 - Azure Disk Encryption for volume encryption ⓘ



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 2

DRAG DROP

You have a private project in Azure DevOps and two users named User1 and User2.

You need to add User1 and User2 to groups to meet the following requirements:

User1 must be able to create a code wiki.

User2 must be able to edit wiki pages.

The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.



Select and Place:

Groups

- Build Administrators
- Contributors
- Project Administrators
- Project Valid Users
- Stakeholders

Answer Area

- User1:
- User2:

Correct Answer:

Groups

Build Administrators
Project Valid Users
Stakeholders

Answer Area

User1:	Project Administrators
User2:	Contributors

Section:

Explanation:

User1: Project Administrators

You must have the permission Create Repository to publish code as wiki. By default, this permission is set for members of the Project Administrators group.

User2: Contributors

Anyone who is a member of the Contributors security group can add or edit wiki pages.

Anyone with access to the team project, including stakeholders, can view the wiki.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/project/wiki/wiki-create-repo>

QUESTION 3

HOTSPOT

Your company has an Azure subscription.

The company requires that all resource group in the subscription have a tag named organization set to a value of Contoso.

You need to implement a policy to meet the tagging requirement.

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

NOTE: Each correct selection is worth one point.

Hot Area:



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

▼
"MicrosoftResources/deployments"
"MicrosoftResources/subscriptions"
"MicrosoftResources/subscriptions/resourceGroups"

▼
"Append",
"Deny",
"DeployIfNotExists",



Answer Area:


```

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

```



Section:

Explanation:

Box 1: " Microsoft.Resources/subscriptions/resourceGroups"

Box 2: "Deny",

Sample - Enforce tag and its value on resource groups

```

},
"policyRule": {
  "if": {
    "allOf": [
      {
        "field": "type",
        "equals": "Microsoft.Resources/subscriptions/resourceGroups"
      },
      {
        "not": {
          "field": "[concat('tags[',parameters('tagName'), ']')]",

```

```
"equals": "[parameters('tagValue')]"
}
}
],
},
"then": {
"effect": "deny"
}
}
}
}
```

References:

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

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



Correct Answer: B, C, E

Section:

Explanation:

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

C:

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

Reference:

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

QUESTION 5

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

Correct Answer: A

Section:

Explanation:

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

Reference:

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

QUESTION 6

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 az400-11566895-main every five hours to an Azure Storage account in your resource group. To complete this task, sign in to the Microsoft Azure portal.

- A. See solution below.

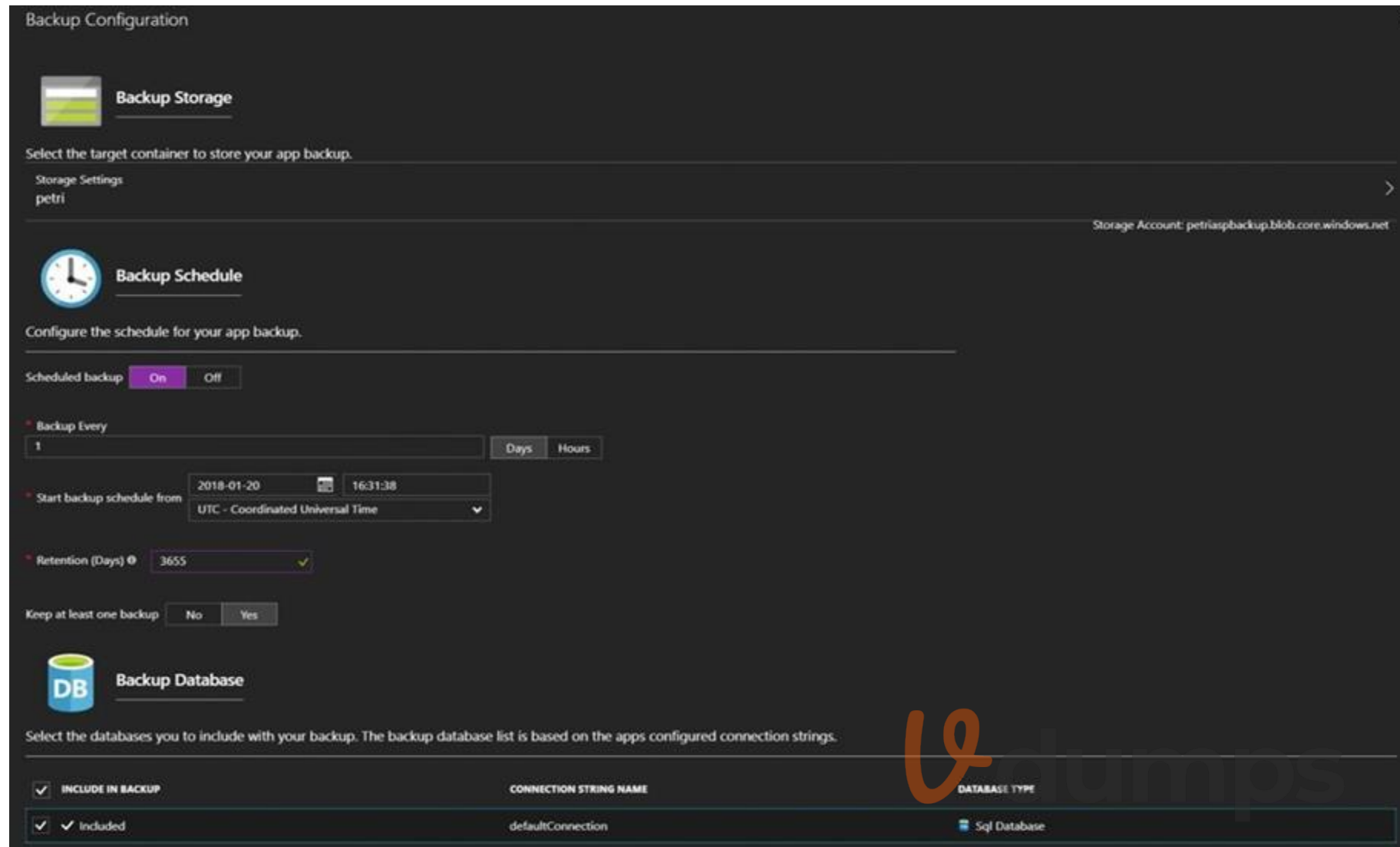
Correct Answer: A

Section:

Explanation:

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

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

You need to configure a virtual machine named VM1 to securely access stored secrets in an Azure Key Vault named az400-11566895-kv. To complete this task, sign in to the Microsoft Azure portal.

A. See solution below.

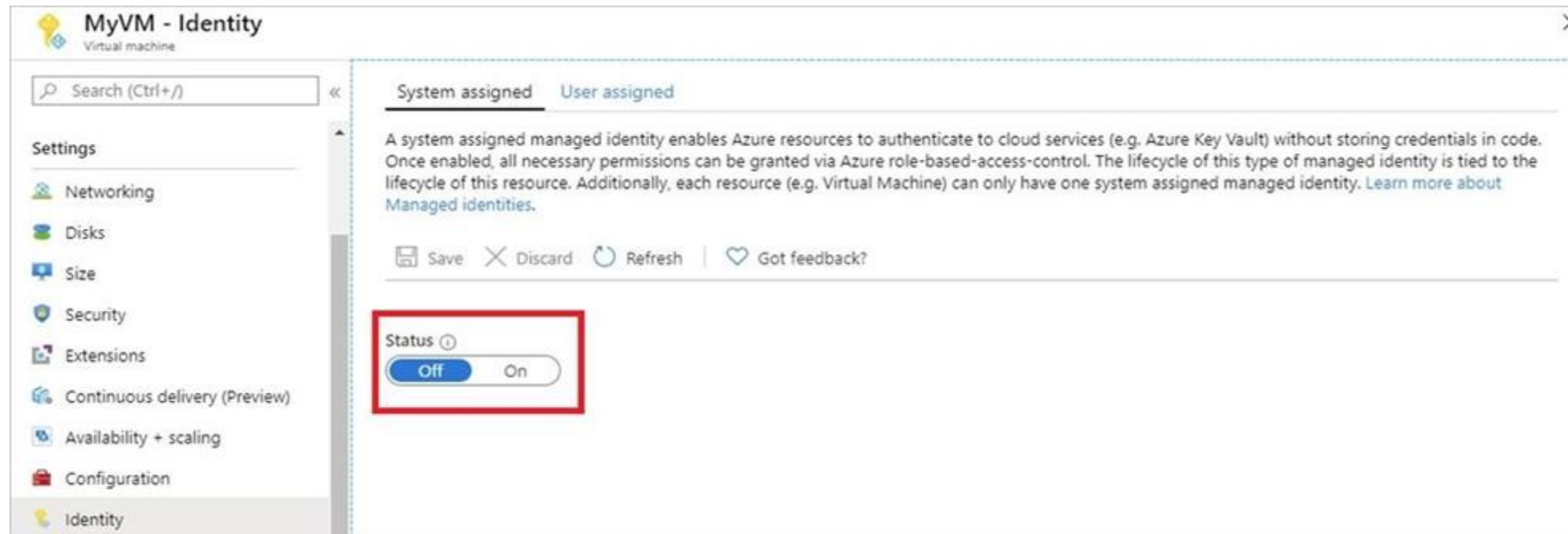
Correct Answer: A

Section:

Explanation:

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

1. Sign in to Azure portal
2. Locate virtual machine VM1.
3. Select Identity
4. Enable the system-assigned identity for VM1 by setting the Status to On.



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 8

HOTSPOT

You manage build and release pipelines by using Azure DevOps. Your entire managed environment resides in Azure.

You need to configure a service endpoint for accessing Azure Key Vault secrets. The solution must meet the following requirements:

Ensure that the secrets are retrieved by Azure DevOps.

Avoid persisting credentials and tokens in Azure DevOps.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Service connection type:

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

Authentication/authorization method for the connection:

	▼
Azure Active Directory OAuth 2.0	
Grant authorization	
Managed Service Identity Authentication	

Answer 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	

Section:

Explanation:

Box 1: Azure Pipelines service connection

Box 2: Managed Service Identity Authentication

The managed identities for Azure resources feature in Azure Active Directory (Azure AD) provides Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code.

Reference:

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

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>



QUESTION 9

HOTSPOT

Your company is creating a suite of three mobile applications.

You need to control access to the application builds. The solution must be managed at the organization level.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Groups to control the build access:

- Active Directory groups
- Azure Active Directory groups
- Microsoft Visual Studio App Center distribution groups

Group type:

- Private
- Public
- Shared

Answer 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

Section:

Explanation:

Box 1: Microsoft Visual Studio App Center distribution Groups

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

Box 2: Shared

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

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

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

QUESTION 10

DRAG DROP

You use GitHub Enterprise Server as a source code repository.

You create an Azure DevOps organization named Contoso.

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

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

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

Select and Place:

Actions

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

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

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

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

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

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

Answer Area



Correct Answer:

Actions

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

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

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

Answer Area

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

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

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



Section:

Explanation:

Step 1: From Developer settings in GitHub Enterprise Server, register a new OAuth app.

If you plan to use OAuth to connect Azure DevOps Services or Azure DevOps Server with your GitHub Enterprise Server, you first need to register the application as an OAuth App

Step 2: Organization settings in Azure DevOps, add an OAuth configuration

Register your OAuth configuration in Azure DevOps Services.

Note:

1. Sign into the web portal for Azure DevOps Services.
2. Add the GitHub Enterprise OAuth configuration to your organization.
3. Open Organization settings>Oauth configurations, and choose Add Oauth configuration.
4. Fill in the form that appears, and then choose Create.

Step 3: From Project Settings in Azure DevOps, add a GitHub connection.

Connect Azure DevOps Services to GitHub Enterprise Server

Choose the Azure DevOps logo to open Projects, and then choose the Azure Boards project you want to configure to connect to your GitHub Enterprise repositories.

Choose (1) Project Settings, choose (2) GitHub connections and then (3) Click here to connect to your GitHub Enterprise organization.

Reference:

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

QUESTION 11

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

You provision an Azure key vault named Keyvault1.

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

What should you do first?

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



Correct Answer: A

Section:

Explanation:

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

Reference:

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

QUESTION 12

You create a Microsoft ASP.NET Core application.

You plan to use Azure Key Vault to provide secrets to the application as configuration data.

You need to create a Key Vault access policy to assign secret permissions to the application. The solution must use the principle of least privilege. Which secret permissions should you use?

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

Correct Answer: B

Section:

Explanation:

Application data plane permissions:

Keys: sign

Secrets: get

Reference:

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

QUESTION 13

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.

Correct Answer: D

Section:

Explanation:

In some cases, you need to bypass policy requirements so you can push changes to the branch directly or complete a pull request even if branch policies are not satisfied. For these situations, grant the desired permission from the previous list to a user or group. You can scope this permission to an entire project, a repo, or a single branch. Manage this permission along with other Git permissions.

Reference:

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

QUESTION 14

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

Correct Answer: A

Section:

Explanation:

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

Reference:

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

QUESTION 15

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.

Correct Answer: D

Section:

Explanation:

Conditional Access is a capability of Azure Active Directory. With Conditional Access, you can implement automated access control decisions for accessing your cloud apps that are based on conditions. Conditional Access policies are enforced after the first-factor authentication has been completed.

Reference:

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

QUESTION 16

You have the following Azure policy.

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



You assign the policy to the Tenant root group.

What is the effect of the policy?

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

Correct Answer: B

Section:

Explanation:

Denies non HTTPS traffic.

QUESTION 17

You have an Azure DevOps organization named Contoso, an Azure DevOps project named Project1, an Azure subscription named Sub1, and an Azure key vault named vault1. You need to ensure that you can reference the values of the secrets stored in vault1 in all the pipelines of Project1. The solution must prevent the values from being stored in the pipelines. What should you do?

- A. Create a variable group in Project1.
- B. Add a secure file to Project1.

- C. Modify the security settings of the pipelines.
- D. Configure the security policy of Contoso.

Correct Answer: A

Section:

Explanation:

Use a variable group to store values that you want to control and make available across multiple pipelines.

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

QUESTION 18

You use WhiteSource Bolt to scan a Node.js application.

The WhiteSource Bolt scan identifies numerous libraries that have invalid licenses. The libraries are used only during development and are not part of a production deployment. You need to ensure that WhiteSource Bolt only scans production dependencies.

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

NOTE: Each correct selection is worth one point.

- A. Run npm install and specify the --production flag.
- B. Modify the WhiteSource Bolt policy and set the action for the licenses used by the development tools to Reassign.
- C. Modify the devDependencies section of the project's Package.json file.
- D. Configure WhiteSource Bolt to scan the node_modules directory only.

Correct Answer: A, C

Section:

Explanation:

A: To resolve NPM dependencies, you should first run "npm install" command on the relevant folders before executing the plugin. C: All npm packages contain a file, usually in the project root, called package.json - this file holds various metadata relevant to the project. This file is used to give information to npm that allows it to identify the project as well as handle the project's dependencies. It can also contain other metadata such as a project description, the version of the project in a particular distribution, license information, even configuration data - all of which can be vital to both npm and to the end users of the package.

Reference: <https://whitesource.atlassian.net/wiki/spaces/WD/pages/34209870/NPM+Plugin> <https://nodejs.org/en/knowledge/getting-started/npm/what-is-the-file-package-json>

QUESTION 19

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

Correct Answer: D

Section:

Explanation:

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

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

Note:

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

1. Black Duck

2. WhiteSource Bolt

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

1. Microsoft Visual SourceSafe
2. PDM
3. SourceGear

Reference:

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

QUESTION 20

You plan to use a NuGet package in a project in Azure DevOps. The NuGet package is in a feed that requires authentication. You need to ensure that the project can restore the NuGet package automatically. What should the project use to automate the authentication?

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

Correct Answer: B

Section:

Explanation:

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

Reference:

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



QUESTION 21

You use Azure Pipelines to manage project builds and deployments.

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

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

Correct Answer: A

Section:

Explanation:

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

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

QUESTION 22

You have an existing project in Azure DevOps.

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

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

Which authentication mechanism should you use?

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

Correct Answer: B

Section:

Explanation:

GitHub App uses the Azure Pipelines identity.

Incorrect Answers:

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

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

QUESTION 23

You plan to provision a self-hosted Linux agent.

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

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

Correct Answer: A

Section:

Explanation:

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

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

QUESTION 24

You are building a Microsoft ASP.NET application that requires authentication.

You need to authenticate users by using Azure Active Directory (Azure AD).

What should you do first?

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

Correct Answer: B

Section:

Explanation:

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

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

QUESTION 25



You have an Azure DevOps organization named Contoso.

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

Supports authentication from Git

Minimizes the need to provide credentials during authentication

What should you recommend?

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

Correct Answer: A

Section:

Explanation:

Personal access tokens (PATs) give you access to Azure DevOps and Team Foundation Server (TFS), without using your username and password directly. These tokens have an expiration date from when they're created. You can restrict the scope of the data they can access. Use PATs to authenticate if you don't already have SSH keys set up on your system or if you need to restrict the permissions that are granted by the credential. Incorrect Answers:

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

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

QUESTION 26

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

Correct Answer: D

Section:

Explanation:

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

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

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

Reference:

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

QUESTION 27

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

Correct Answer: B

Section:

Explanation:

Instead implement continuous integration.

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

Reference:

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

QUESTION 28

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.

- A. See solution below.

Correct Answer: A

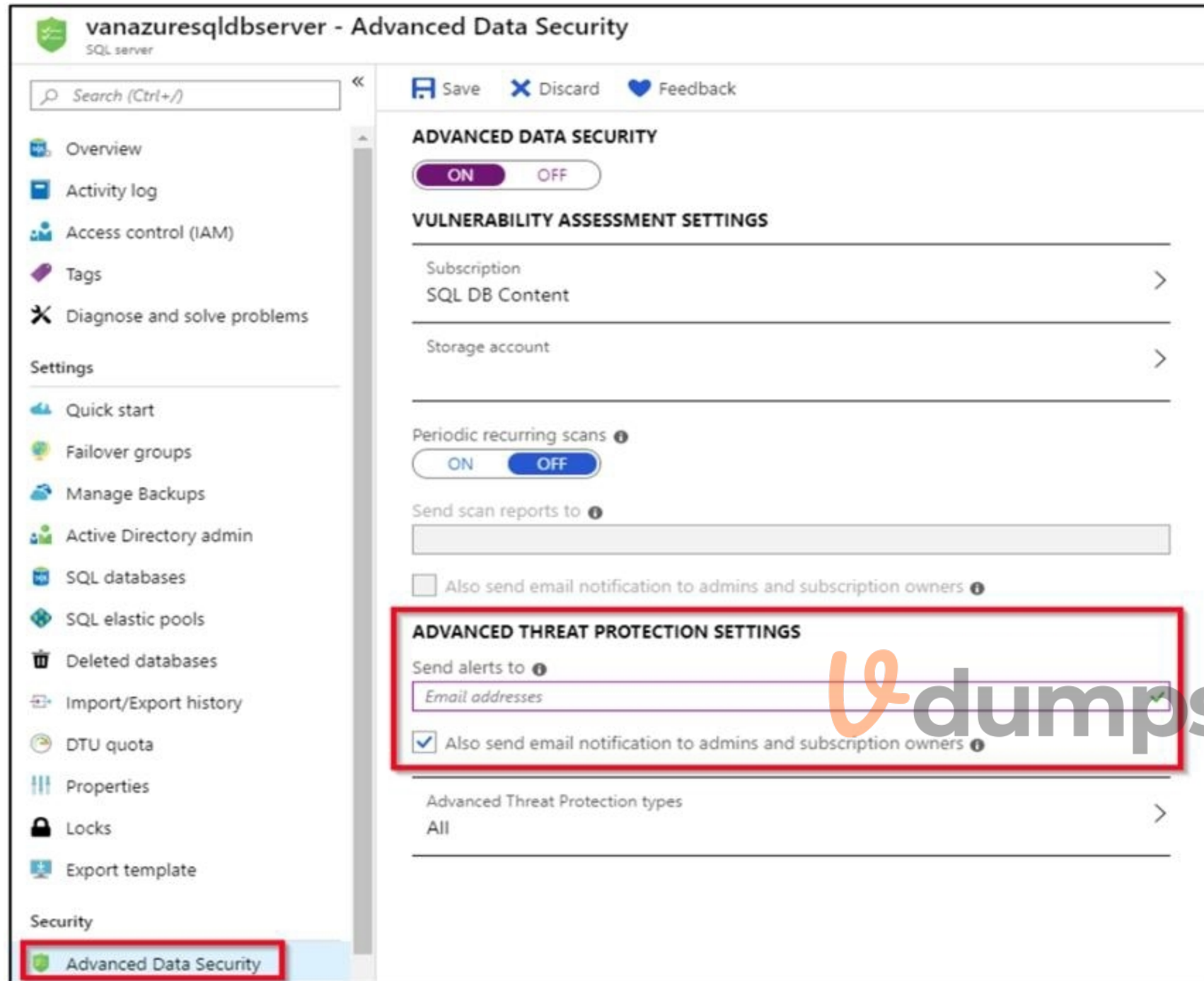
Section:

Explanation:

Set up Advanced Threat Protection in the Azure portal

1. Sign into the Azure portal.
2. Navigate to the configuration page of the server you want to protect. In the security settings, select Advanced Data Security.
3. On the Advanced Data Security configuration page:





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 29

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

Correct Answer: B

Section:

Explanation:

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

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

Reference:

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

QUESTION 30

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

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

What should you use?

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

Correct Answer: C

Section:

Explanation:

Secure and Manage Open Source Software

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

Note:

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

1. Black Duck
2. WhiteSource Bolt

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

1. OWASP ZAP
2. PDM
3. SourceGear

Reference:

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

QUESTION 31

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

Correct Answer: C

Section:

Explanation:

Secure and Manage Open Source Software

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

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

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

QUESTION 32

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

You need to identify which certificate file you require to distribute the new release from App Center. Which file type should you upload to App Center?

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

Correct Answer: C

Section:

Explanation:

A successful iOS device build will produce an ipa file. In order to install the build on a device, it needs to be signed with a valid provisioning profile and certificate. To sign the builds produced from a branch, enable code signing in the configuration pane and upload a provisioning profile (.mobileprovision) and a valid certificate (.p12), along with the password for the certificate.

Reference:

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

QUESTION 33

SIMULATION

You need to prepare a network security group (NSG) named az400-9940427-nsg1 to host an Azure DevOps pipeline agent. The solution must allow only the required outbound port for Azure DevOps and deny all other inbound and outbound access to the Internet.

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

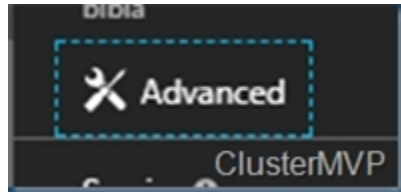
- A. See solution below.

Correct Answer: A

Section:

Explanation:

1. Open Microsoft Azure Portal and Log into your Azure account.
2. Select network security group (NSG) named az400-9940427-nsg1
3. Select Settings, Outbound security rules, and click Add
4. Click Advanced



5. Change the following settings:

Destination Port range: 8080

Protocol: TCP

Action: Allow

Note: By default, Azure DevOps Server uses TCP Port 8080.

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 34

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.



Correct Answer: B

Section:

Explanation:

When you connect to a Get repository from your Get client for the first time, the credential manager prompts for credentials. Provide your Microsoft account or Azure AD credentials. Note: Git Credential Managers simplify authentication with your Azure Repos Git repositories. Credential managers let you use the same credentials that you use for the Azure DevOps Services web portal. Credential managers support multi-factor authentication through Microsoft account or Azure Active Directory (Azure AD). Besides supporting multi-factor authentication with Azure Repos, credential managers also support two-factor authentication with GitHub repositories.

Reference:

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

QUESTION 35

You have an Azure DevOps project named Project1 and an Azure subscription named Sub1.

You need to prevent releases from being deployed unless the releases comply with the Azure Policy rules assigned to Sub1. What should you do in the release pipeline of Project1?

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

Correct Answer: A

Section:

Explanation:

You can check policy compliance with gates.

You can extend the approval process for the release by adding a gate. Gates allow you to configure automated calls to external services, where the results are used to approve or reject a deployment. You can use gates to ensure that the release meets a wide range of criteria, without requiring user intervention.

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

QUESTION 36

You have an Azure DevOps project that contains a build pipeline. The build pipeline uses approximately 50 open source libraries. You need to ensure that all the open source libraries comply with your company's licensing standards. Which service should you use?

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

Correct Answer: C

Section:

Explanation:

WhiteSource provides WhiteSource Bolt, a lightweight open source security and management solution developed specifically for integration with Azure DevOps and Azure DevOps Server. Note: WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.

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

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

QUESTION 37

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

Correct Answer: A

Section:

Explanation:

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:

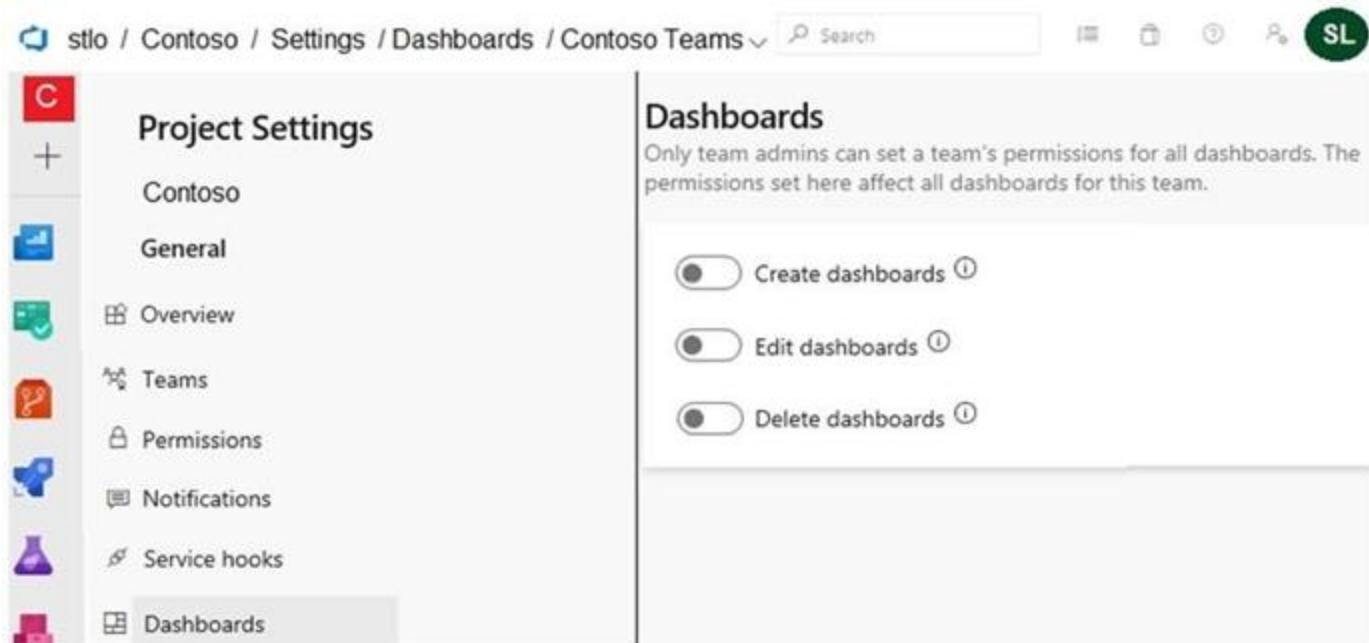
<https://octopus.com/docs/packaging-applications>

QUESTION 38

HOTSPOT

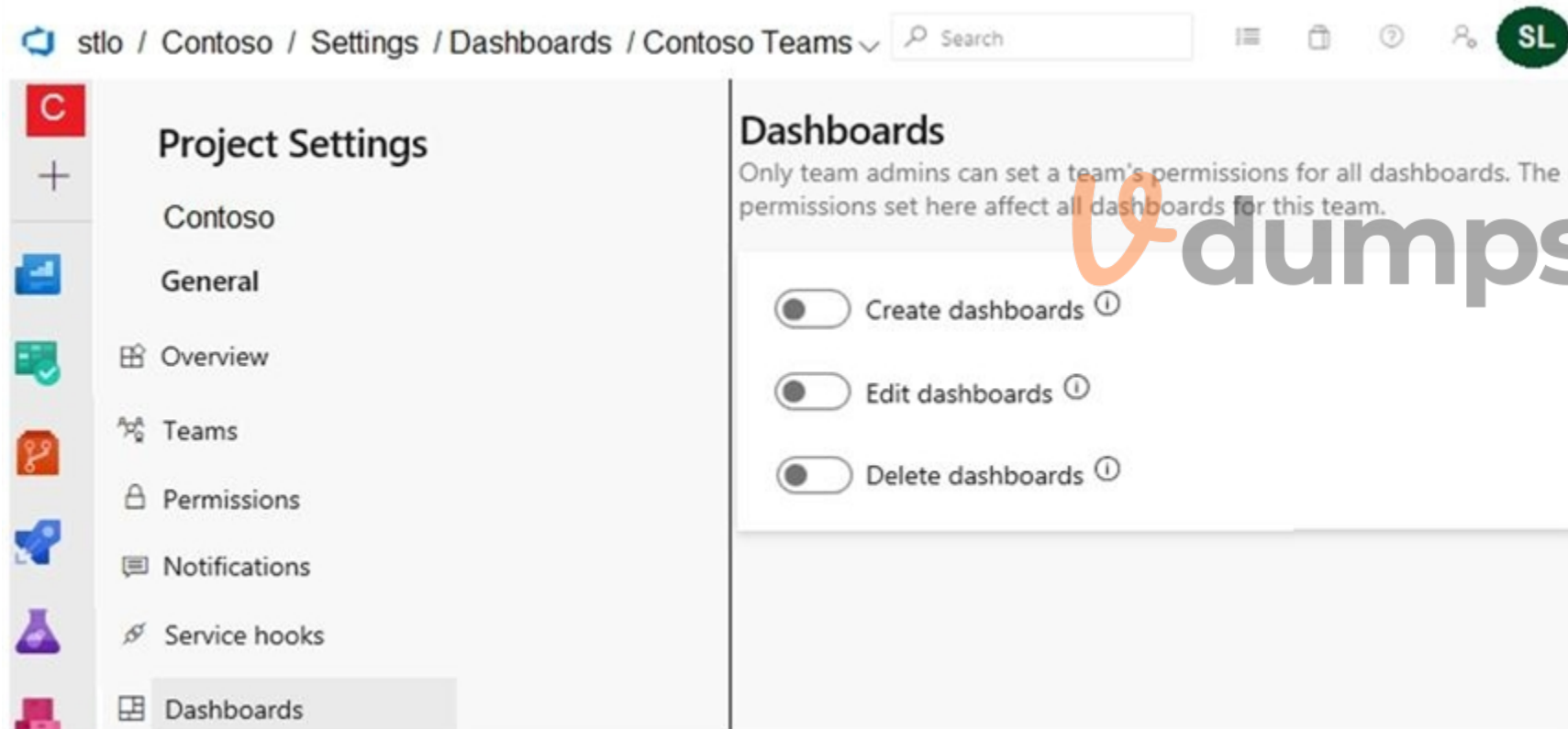
You have a project in Azure DevOps that has three teams as shown in the Teams exhibit. (Click the Teams tab.)





You create a new dashboard named Dash1.

You configure the dashboard permissions for the Control 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.	<input type="radio"/>	<input type="radio"/>
Contoso Team can view Dash1.	<input type="radio"/>	<input type="radio"/>
Project administrators can create new dashboards.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

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

Section:

Explanation:

Reference:

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

QUESTION 39

DRAG DROP

Your company has a project in Azure DevOps.

You plan to create a release pipeline that will deploy resources by using Azure Resource Manager templates. The templates will reference secrets stored in Azure Key Vault.

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

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

NOTE: Each correct selection is worth one point.

Select and Place:

Configurations

Answer Area

A Key Vault access policy

Enable key vaults for template deployment by using:

A Key Vault advanced access policy

Restrict access to the secrets in Key Vault by using:

RBAC

Correct Answer:

Configurations

Answer Area

A Key Vault advanced access policy

Enable key vaults for template deployment by using:

RBAC

Restrict access to the secrets in Key Vault by using:

A Key Vault access policy

Section:

Explanation:

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

QUESTION 40

DRAG DROP

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

Use a project agent pool when authoring build or release pipelines.

View the agent pool and agents of the organization.

Use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Select and Place:



Roles

- Administrator
- Reader
- Service Account
- User

Answer Area

Organization:
Project:

Correct Answer:

Roles

- Administrator
-
- Service Account
-

Answer Area

Organization:
Project:



Section:

Explanation:

References: <https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues?view=azure-devops&tabs=yaml%2Cbrowser>

QUESTION 41

DRAG DROP

Your company has an Azure subscription named Subscription1. Subscription1 is associated to an Azure Active Directory tenant named contoso.com.

You need to provision an Azure Kubernetes Services (AKS) cluster in Subscription1 and set the permissions for the cluster by using RBAC roles that reference the identities in contoso.com.

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

Select and Place:

Answer Area

Objects

a system-assigned managed identity

a cluster

an application registration in contoso.com

an RBAC binding

Three empty red-bordered boxes for the answer area.

Correct Answer:

Answer Area

Objects

an application registration in contoso.com

Three red-bordered boxes for the answer area. The first box contains "a cluster" and has a large watermark "Vdumps" overlaid on it. The second box contains "a system-assigned managed identity". The third box contains "an RBAC binding".

Section:

Explanation:

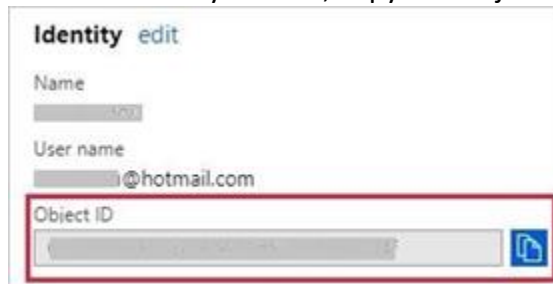
Step 1: Create an AKS cluster

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.



The screenshot shows the 'Identity edit' form with the following fields:

- Name: [Redacted]
- User name: [Redacted]@hotmail.com
- Object ID: [Redacted]

The 'Object ID' field is highlighted with a red border.

Step 3: a RBAC binding

Reference:

<https://docs.microsoft.com/en-us/azure/developer/ansible/aks-configure-rbac>

QUESTION 42

DRAG DROP

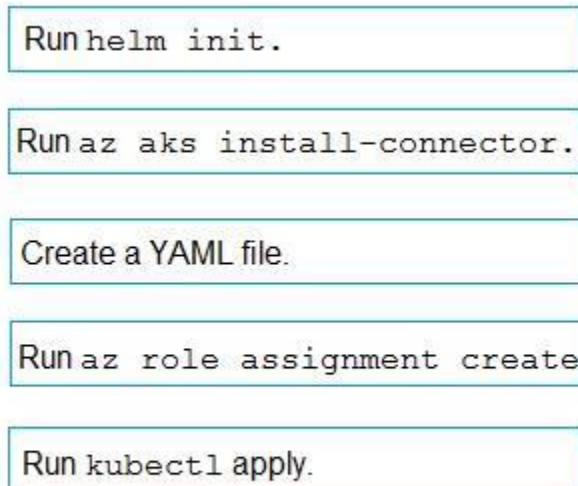
You have an Azure Kubernetes Service (AKS) implementation that is RBAC-enabled.

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:



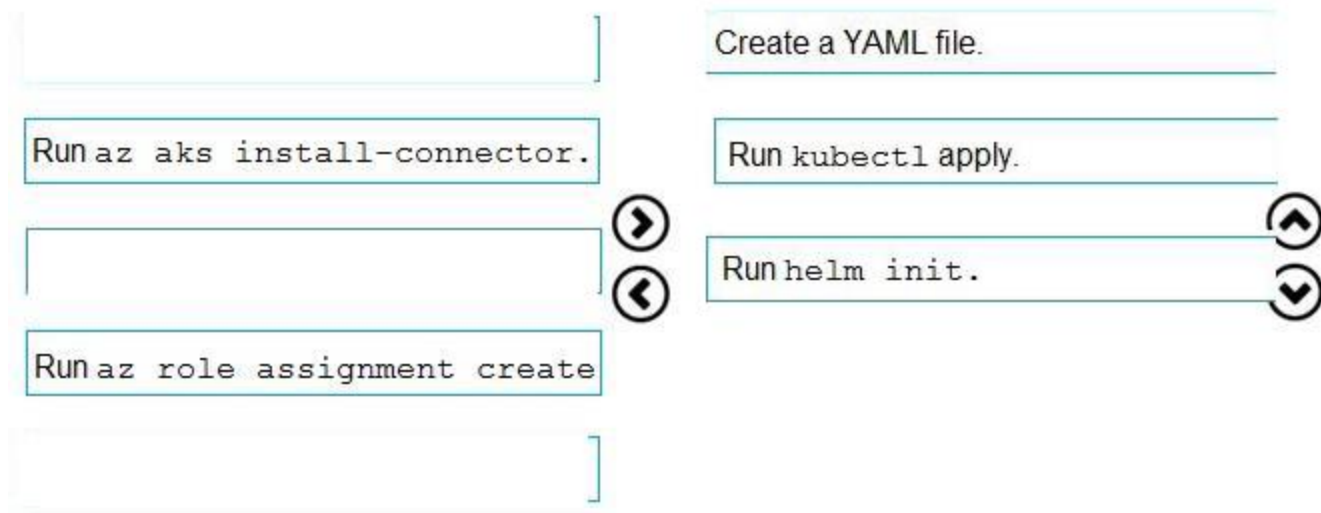
The screenshot shows the 'Select and Place' interface with the following actions in a list:

- Run `helm init`.
- Run `az aks install-connector`.
- Create a YAML file.
- Run `az role assignment create`
- Run `kubectl apply`.

Each action is in a box with a right-pointing arrow on its right side. The 'Create a YAML file.' box has a left-pointing arrow on its left side. The 'Run `az role assignment create`' box has a right-pointing arrow on its right side.

Correct Answer:





Section:

Explanation:

Step 1: Create a YAML file.

If your AKS cluster is RBAC-enabled, you must create a service account and role binding for use with Tiller. To create a service account and role binding, create a file named rbac-virtual-kubelet.yaml

Step 2: Run kubectl apply.

Apply the service account and binding with kubectl apply and specify your rbac-virtual-kubelet.yaml file.

Step 3: Run helm init.

Configure Helm to use the tiller service account:

```
helm init --service-account tiller
```

You can now continue to installing the Virtual Kubelet into your AKS cluster.

References: <https://docs.microsoft.com/en-us/azure/aks/virtual-kubelet>



QUESTION 43

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:

Files

- The .npmrc file in the project
- The npmrc file in the user's home folder
- The Package.json file in the project
- The Project.json file in the project

Answer Area

Feed registry information:

Credentials:

Correct Answer:

Files

-
-
- The Package.json file in the project
- The Project.json file in the project

Answer Area

Feed registry information:

Credentials:

Section:

Explanation:

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

Feed registry information: The .npmrc file in the project

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

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

On your development machine, you will also have a .npmrc in \$home for Linux or Mac systems or \$env.HOME for win systems. This .npmrc should contain credentials for all of the registries that you need to connect to. The NPM client will look at your project's .npmrc, discover the registry, and fetch matching credentials from \$home/.npmrc or \$env.HOME/.npmrc.

References:

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

QUESTION 44

HOTSPOT

You have an Azure DevOps project that contains a build pipeline. The build pipeline uses approximately 50 open source libraries.

You need to ensure that the project can be scanned for known security vulnerabilities in the open source libraries.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Object to create:

A build task
A deployment task
An artifacts repository

Service to use:

WhiteSource Bolt
Bamboo
CMake
Chef



Answer Area:

Answer Area

Object to create:

A build task
A deployment task
An artifacts repository

Service to use:

WhiteSource Bolt
Bamboo
CMake
Chef



Section:

Explanation:

Box 1: A Build task

Trigger a build

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

1. Go to Builds section under Pipelines tab, select the build definition WhiteSourceBolt and click on Queue to trigger a build. 2. To view the build in progress status, click on ellipsis and select View build results.

Box 2: WhiteSource Bolt

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

References:

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

QUESTION 45

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

The company identifies security as one of the highest priorities.

You need to recommend a solution to minimize the likelihood that infrastructure credentials will be leaked. What should you recommend?

- A. Add a Run Inline Azure PowerShell task to the pipeline.
- B. Add a PowerShell task to the pipeline and run Set-AzureKeyVaultSecret.
- C. Add an Azure Key Vault task to the pipeline.
- D. Add Azure Key Vault references to Azure Resource Manager templates.

Correct Answer: B

Section:

Explanation:

Azure Key Vault provides a way to securely store credentials and other keys and secrets.

The Set-AzureKeyVaultSecret cmdlet creates or updates a secret in a key vault in Azure Key Vault.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecret>

QUESTION 46

SIMULATION

You need to ensure that an Azure web app named az400-9940427-main can retrieve secrets from an Azure key vault named az400-9940427-kv1 by using a system managed identity. The solution must use the principle of least privilege.

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

A. See solution below.

Correct Answer: A

Section:

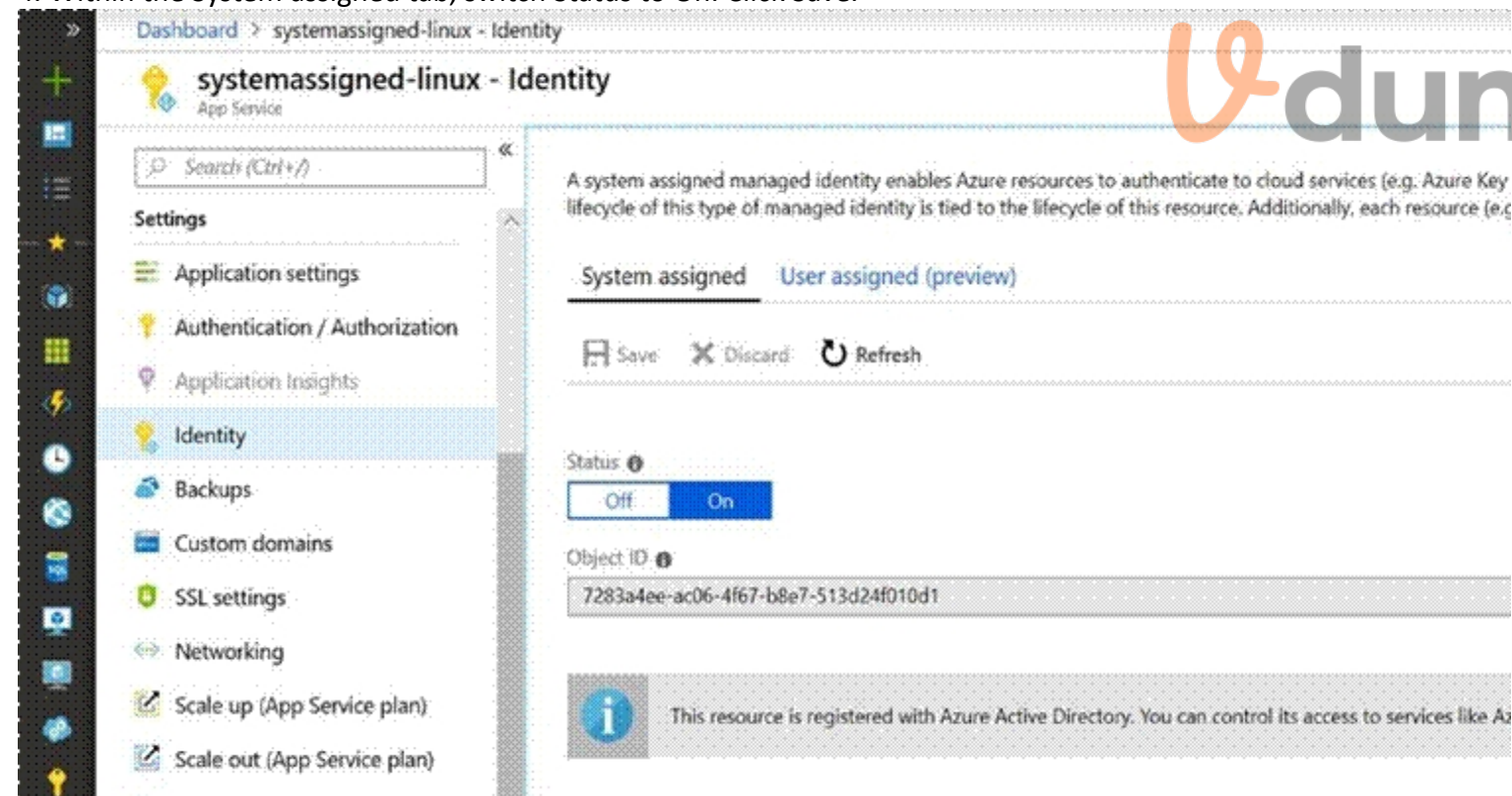
Explanation:

1. In Azure portal navigate to the az400-9940427-main app.

2. Scroll down to the Settings group in the left navigation.

3. Select Managed identity.

4. Within the System assigned tab, switch Status to On. Click Save.



Reference:

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

QUESTION 47

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

Correct Answer: B

Section:

Explanation:

Instead use implement continuous integration.

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

Reference:

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

QUESTION 48

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

After you answer a question-in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You plan to update the Azure DevOps strategy of your company.

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

Licensing violations Prohibited libraries

Solution: You implement automated security testing.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

Instead use implement continuous integration.

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

Reference:

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

QUESTION 49

DRAG DROP

You plan to use Azure Kubernetes Service (AKS) to host containers deployed from images hosted in a Docker Trusted Registry.

You need to recommend a solution for provisioning and connecting to AKS. The solution must ensure that AKS is RBAC-enabled and uses a custom service principal.

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

Select and Place:

Commands

Answer Area

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



Correct Answer:

Commands

Answer Area

- az role assignment create
- az aks get-credentials
-
-
-



- az aks create
- az ad sp create-for-rbac
- kubectl create



Section:

Explanation:

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>
```

References:

<https://thorsten-hans.com/how-to-use-private-azure-container-registry-with-kubernetes>

QUESTION 50

DRAG DROP

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

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

Select and Place:

Actions

Create a service principal in Azure Active Directory.

In Project1, create a service connection.

In Pipeline1, authorize the service connection.

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

In Project1, configure permissions.

In Pipeline1, create a variable.

Answer Area



Correct Answer:

Actions

In Pipeline1, authorize the service connection.

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

In Pipeline1, create a variable.

Answer Area

Create a service principal in Azure Active Directory.

In Project1, create a service connection.

In Project1, configure permissions.

Section:

Explanation:

Reference:

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

QUESTION 51

DRAG DROP

You need to increase the security of your team's development process.

Which type of security tool should you recommend for each stage of the development process? To answer, drag the appropriate security tools to the correct stages. Each security tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Security Tools

Answer Area

Penetration testing	Pull request:	
Static code analysis	Continuous integration:	
Threat modeling	Continuous delivery:	



Correct Answer:

Security Tools

Answer Area

	Pull request:	Threat modeling
	Continuous integration:	Static code analysis
	Continuous delivery:	Penetration testing

Section:

Explanation:

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>

Exam G

QUESTION 1

You have an Azure solution that contains a build pipeline in Azure Pipelines.

You experience intermittent delays before the build pipeline starts.

You need to reduce the time it takes to start the build pipeline.

What should you do?

- A. Enable self-hosted build agents.
- B. Create a new agent pool.
- C. Split the build pipeline into multiple stages.
- D. Purchase an additional parallel job.

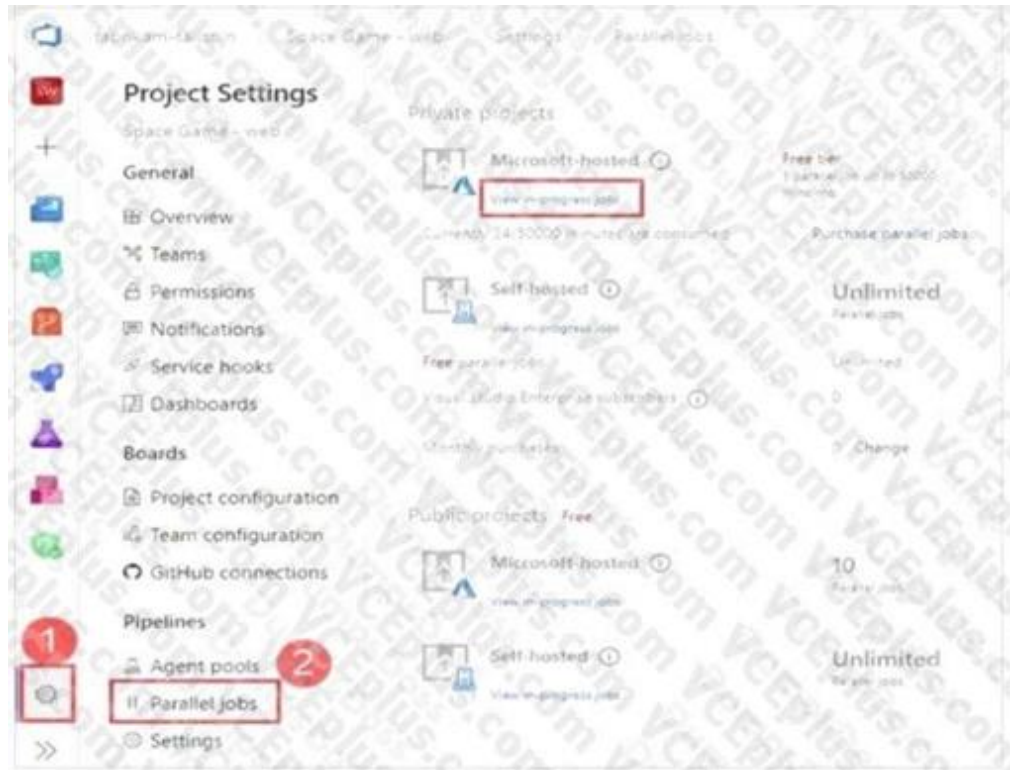
Correct Answer: D

Section:

Explanation:

We need to ensure that resources are available without a startup delay. We don't have enough concurrency. To check how much concurrency you have:

To check your limits, navigate to Project settings, Parallel jobs.



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

QUESTION 2

You are creating a YAML-based Azure pipeline to deploy an Azure Data factory instance that has the following requirements;

- If a Data Factory instance exists already, the instance must be overwritten.
- No other resources in a resource group named Fabrikam must be affected.

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

NOTE: Each correct selection is worth one point.

Answer Area

```

steps:
- task: AzureResourceManagerTemplateDeployment@3
  inputs:
    deploymentScope: 'Resource Group'
    azureResourceManagerConnection: 'Fabrikam Corporate(a41fb3ed-a2aa-42f0-a7ac-8fcc6ef0c5db)'
    subscriptionId: 'a41de0ed-a2aa-42f0-a7ac-8fcc6ef0c5db'
    action: 
    resourceGroupName: 'Fabrikam'
    location: 'West US'
    templateLocation: 'Linked artifact'
    deploymentMode: 

```

A.

```
steps:
- task: AzureResourceManagerTemplateDeployment@3
  inputs:
    deploymentScope: 'Resource Group'
    azureResourceManagerConnection: 'Fabrikam Corporate(a41fb3ed-a2aa-42f0-a7ac-8fcc6ef0c5db)'
    subscriptionId: 'a41de0ed-a2aa-42f0-a7ac-8fcc6ef0c5db'
    action: 'Create Or Update Resource Group'
    resourceGroupName: 'Fabrikam'
    location: 'West US'
    templateLocation: 'Linked artifact'
    deploymentMode: 'Incremental'
```

Correct Answer: A

Section:

QUESTION 3

DRAG DROP

You have an Azure Kubernetes Service (AKS) pod that hosts an app named App1.

You need to configure the AKS container to restart automatically if the container stops responding. The solution must check the status of App1 once every three seconds.

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

NOTE: Each correct selection is worth one point.

Select and Place:



Values

Answer Area

```
apiVersion: 2019-12-01
location: eastus
name: App1
properties:
  containers:
  - name: container1
    properties:
      image: mycompany/myImage:1.0.1
    ports: []
    resources:
      resources:
        requests:
          cpu: 1.0
          memoryInGB: 1.5
          
        httpGet:
          path: /
          port: 8080
          
          timeoutSeconds: 1
    osType: linux
    restartPolicy: 
tags: null
type: Microsoft.ContainerInstance/containerGroups
...
```

Correct Answer:

Values

Always

InitialDelaySeconds

livenessProbe

Never

successThreshold

Answer Area

```
apiVersion: 2019-12-01
location: eastus
name: App1
properties:
  containers:
    - name: container1
      properties:
        image: mycompany/myImage:1.0.1
        ports: []
        resources:
          resources:
            requests:
              cpu: 1.0
              memoryInGB: 1.5
        readinessProbe:
          httpGet:
            path: /
            port: 8080
            value: 1
            timeoutSeconds: 1
        osType: linux
        restartPolicy: periodSeconds
      tags: null
    type: Microsoft.ContainerInstance/containerGroups
  ...
```

Section:
Explanation:

Values

Answer Area

```

apiVersion: 2019-12-01
location: eastus
name: App1
properties:
  containers:
  - name: container1
    properties:
      image: mycompany/myimage:1.0.1
      ports: []
      resources:
      resources:
      requests:
        cpu: 1.0
        memoryInGB: 1.5
      readinessProbe
      httpGet:
        path: /
        port: 8080
        Value: 3
        timeoutSeconds: 1
      osType: linux
      restartPolicy: periodSeconds
    tags: null
    type: Microsoft.ContainerInstance/containerGroups
    ...

```

QUESTION 4

HOTSPOT

You plan to use Desired State Configuration (DSC) to maintain the configuration state of virtual machines that run Windows Server.

You need to perform the following:

Install Internet Information Services (IIS) on the virtual machines. Update the default home page of the IIS web server. How should you configure the DSC configuration file? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



```
Configuration WebServerConfig {
  Import-DscResource -ModuleName PsDesiredStateConfiguration
  Node 'localhost' {
```

- Service
- WindowsFeature
- WindowsOptionalFeature
- WindowsProcess

```
WebServer {
```

```
  Ensure = "Present"
  Name = "Web-Server"
```

```
DefaultHomePage {
```

- Archive
- File
- Package
- Script

```
  Ensure = 'Present'
  SourcePath = '\\server1
  \DSCResources\web\index.htm'
  DestinationPath = 'c:\inetpub\wwwroot'
```



Answer Area:

```

Configuration WebServerConfig {
  Import-DscResource -ModuleName PsDesiredStateConfiguration
  Node 'localhost' {
    WebServer {
      Service
      WindowsFeature
      WindowsOptionalFeature
      WindowsProcess

      Ensure = "Present"
      Name = "Web-Server"
    }

    DefaultHomePage {
      Archive
      File
      Package
      Script

      Ensure = 'Present'
      SourcePath = '\\server1
\DSCResources\web\index.htm'
      DestinationPath = 'c:\inetpub\wwwroot'
    }
  }
}

```



Section:

Explanation:

Box 1: WindowsFeature Example:

```

Configuration WebsiteTest {
  # Import the module that contains the resources we're using.
  Import-DscResource -ModuleName PsDesiredStateConfiguration
  # The Node statement specifies which targets this configuration will be applied to.
  Node 'localhost' {
    # The first resource block ensures that the Web-Server (IIS) feature is enabled.
    WindowsFeature WebServer {
      Ensure = "Present"
      Name = "Web-Server" }
  }
}

```

Box 2: File

Example continued:

```

# The second resource block ensures that the website content copied to the website root folder.
File WebsiteContent { Ensure = 'Present'
  SourcePath = 'c:\test\index.htm'
  DestinationPath = 'c:\inetpub\wwwroot' }

```

Reference: <https://docs.microsoft.com/en-us/powershell/scripting/dsc/quickstarts/website-quickstart>

QUESTION 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.

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

The build must access an on-premises dependency management system.

The build outputs must be stored as Server artifacts in Azure DevOps. The source code must be stored in a get repository in Azure DevOps.

Solution: Configure the build pipeline to use a Microsoft-hosted agent pool running the Windows Server 2022 with Visual Studio 2022 image. Include the Java Tool Installer task in the build pipeline.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

QUESTION 6

You have a project in Azure DevOps.

You create the following YAML template named Template1.yml.

steps:

- script: npm install
- script: yarn install
- script: npm run compile

You create the following pipeline named File1.yml.

parameters: usersteps: - task: MyTask@1

- script: echo Done

You need to ensure that Template1.yml runs before File1.yml.

How should you update File1.yml?

- A. parameters: usersteps: extends: template: template1.yml
- task: MyTask@1 - script: echo Done
- B. template: template1.yml parameters: usersteps:
- task: MyTask@1 - script: echo Done
- C. extends: template: template1.yml parameters: usersteps:
- task: MyTask@1 - script: echo Done
- D. parameters: usersteps: - template: template1.yml
- task: MyTask@1 - script: echo Done

Correct Answer: C

Section:

Explanation:

Azure Pipelines offers two kinds of templates: includes and extends. Included templates behave like #include in C++: it's as if you paste the template's code right into the outer file, which references it. To continue the C++ metaphor, extends templates are more like inheritance: the template provides the outer structure of the pipeline and a set of places where the template consumer can make targeted alterations.

Example: extends: template: template.yml@templates parameters: usersteps:

- script: echo This is my first step - script: echo This is my second step

Reference: <https://docs.microsoft.com/en-us/azure/devops/pipelines/security/templates>



QUESTION 7

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 get repository for Project1. The solution must meet the following requirements:

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

Select and Place:

Actions	Answer Area
Perform a custom installation of Git for Windows that includes Git Virtual File System (GVFS).	1
Configure personal access token (PAT)-based authentication.	2
Perform a custom installation of Git for Windows that includes Git Large File Storage (LFS).	3
Configure SSH key-based authentication.	
Configure Git Large File Storage (LFS) file tracking.	

Correct Answer:

Actions	Answer Area
Perform a custom installation of Git for Windows that includes Git Virtual File System (GVFS).	1 Perform a custom installation of Git for Windows that includes Git Large File Storage (LFS).
Configure personal access token (PAT)-based authentication.	2 Configure SSH key-based authentication.
	3 Configure Git Large File Storage (LFS) file tracking.

Section:

Explanation:

Actions	Answer Area
Perform a custom installation of Git for Windows that includes Git Virtual File System (GVFS).	1 Perform a custom installation of Git for Windows that includes Git Large File Storage (LFS).
Configure personal access token (PAT)-based authentication.	2 Configure SSH key-based authentication.
	3 Configure Git Large File Storage (LFS) file tracking.

QUESTION 8

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

You need to identify all the changes made between versions 1.4.16 and 1.6.12 of the source code.

How should you complete the get command? To answer, select the appropriate options in the answer area. get _____ | helper-script > changes.txt

NOTE: Each correct selection is worth one point.

Answer Area

```
git [ ] [ ] | helper-script > changes.txt
```

A. `get diff v1.4.16 v1.6.12 | helper-script > changes.txt`

Correct Answer: A

Section:

Explanation:

This command will compare the changes made between versions 1.4.16 and 1.6.12 of the source code in your GitHub repository, pipe the output through the helper-script and save the result to a file called "changes.txt". Please note that, this command assumes that you have a helper-script that can handle get diff output as an input and processes it further. It is not a default get command.

QUESTION 9

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 Azure Marketplace.

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

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

Correct Answer: C

Section:

QUESTION 10

DRAG DROP

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

- The lead developer must be able to create repositories, manage permissions, manage policies, and contribute to the repository.
- Developers must be able to contribute to the repository and create branches, but NOT bypass policies when pushing builds.
- Project managers must only be able to view the repository.
- The principle of least privilege must be used.

You create a new Azure DevOps project team for each role.

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

NOTE: Each correct selection is worth one point.

Select and Place:



Azure DevOps groups

- Build Administrators
- Contributors
- Project Administrators
- Project Collection Administrators
- Project Collection Valid Users

Answer Area

Project manager:

Lead developer:

Developer:

Correct Answer:**Azure DevOps groups**

- Build Administrators
-
-
-
- Project Collection Valid Users

Answer Area

Project manager:

Lead developer:

Developer:

**Section:****Explanation:****QUESTION 11**

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

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

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

The build must access an on-premises dependency management system.

The build outputs must be stored as Server artifacts in Azure DevOps. The source code must be stored in a get repository in Azure DevOps.

Solution: Configure the build pipeline to use a Microsoft-hosted agent pool running a Linux image. Include the Java Tool Installer task in the build pipeline.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A**Section:****Explanation:**

To run your jobs, you'll need at least one agent. A Linux agent can build and deploy different kinds of apps, including Java and Android apps.

If your pipelines are in Azure Pipelines and a Microsoft-hosted agent meets your needs, you can skip setting up a private Linux agent.

The Azure Pipelines agent pool offers several virtual machine images to choose from, each including a broad range of tools and software. We support Ubuntu, Red Hat, and CentOS.

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

QUESTION 12

DRAG DROP

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

You generate a risk graph for the project.

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

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

NOTE: Each correct selection is worth one point.

Select and Place:

Elements

- Link color
- Link length
- Link width
- Node color

Answer Area

- Number of dependencies
- Risk level

Correct Answer:

Elements

-
- Link length
-
- Node color

Answer Area

- Number of dependencies
- Risk level

Section:

Explanation:

Box 1: Link width

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

Box 2: Link color

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

QUESTION 13

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

What should you do?

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

Correct Answer: A

Section:

Explanation:

Don't set secret variables in your YAML file. Operating systems often log commands for the processes that they run, and you wouldn't want the log to include a secret that you passed in as an input. Use the script's environment or map the variable within the variables block to pass secrets to your pipeline.

Incorrect Answers:

B: Never pass secrets on the command line.

C: Adding a prefix does not make the variable a secret. The `issecret` property makes it secret but does not prevent logging of the secret. D: Never echo secrets as output.

Reference:

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

QUESTION 14

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. Participating
- B. Automatically watch repositories
- C. Automatically watch teams
- D. Watching

Correct Answer: B, D

Section:

QUESTION 15

LAB 3

You need to ensure that an Azure Web App named `az400-38443478-main` supports rolling upgrades. The solution must ensure that only 10 percent of users who connect to `az400-38443478-main` use updated versions of the app. The solution must minimize administrative effort.

- A. See the solution below in explanation

Correct Answer: A

Section:

Explanation:

To ensure that your Azure Web App named `az400-38443478-main` supports rolling upgrades and only 10 percent of users connect to the updated version of the app, you can use deployment slots with the following steps:



Create a Deployment Slot:

Navigate to the Azure Portal.

Go to your Web App az400-38443478-main.

Select Deployment slots in the menu.

Click on Add Slot.

Name the slot (e.g., staging) and if needed, clone settings from the production slot.

Configure the Traffic Percentage:

In the Deployment Slots menu, you will see a column for Traffic %.

Set the traffic percentage to 10% for the staging slot1.

This will route only 10% of the traffic to the updated version of the app in the staging slot.

Deploy the Updated App to the Staging Slot:

Deploy your updated application to the staging slot.

Test the application in the staging slot to ensure it's working as expected.

Complete the Rolling Upgrade:

Once you're satisfied with the performance and stability of the app in the staging slot, you can gradually increase the percentage of traffic until you're ready to swap with the production slot.

To swap slots, go to the Deployment slots menu and click on Swap with the production slot.

By using deployment slots, you can achieve rolling upgrades with minimal administrative effort, as it allows you to test the new version on a subset of users before fully releasing it. Remember to adjust the traffic percentage and monitor the application's performance throughout the process.

QUESTION 16

LAB 4

You need to configure a virtual machine template in a DevTest Labs environment named az400-38443478-dtl1. The operating system must be based on Windows Server 2016 Datacenter. Virtual machines created from the DevTest Lab must include the Selenium tool and the Google Chrome browser.

A. See the solution below in explanation



Correct Answer: A

Section:

Explanation:

To configure a virtual machine template in your DevTest Labs environment named az400-38443478-dtl1 with Windows Server 2016 Datacenter that includes the Selenium tool and the Google Chrome browser, follow these steps:

Create a Custom Image with Windows Server 2016 Datacenter:

In the Azure Portal, go to your DevTest Lab az400-38443478-dtl1.

Navigate to Configuration and policies > Custom images.

Use an existing VM or create a new one with Windows Server 2016 Datacenter.

After setting up the VM, capture it to create a custom image1.

Install Selenium and Google Chrome on the VM:

Connect to the VM via RDP.

Download and install the Selenium WebDriver for your preferred programming language from the official Selenium website2.

For Google Chrome, download the offline installer from the official website and install it on the VM3.

Generalize the VM:

Run the sysprep command to generalize the VM, which prepares it to be used as a template.

Shut down the VM after sysprep completes.

Capture the Generalized VM to Create a Template:

In the Azure Portal, navigate to the VM and select Capture.

Provide the required details and create the image.

Add Selenium and Google Chrome Artifacts to the Template:

Go back to the DevTest Lab az400-38443478-dtl1.

Select Artifacts and add Selenium and Google Chrome artifacts to the template.

Ensure these artifacts are configured to install during the VM creation process.

Create VMs from the Template:

Now, when you create a new VM in the DevTest Lab, select the custom image you created.

The VM will be provisioned with Windows Server 2016 Datacenter, and the Selenium tool and Google Chrome browser will be installed automatically.

By following these steps, you can ensure that all virtual machines created from this template in your DevTest Lab will have the required operating system, tools, and browser installed. Remember to replace placeholder names with the actual names of your resources where necessary.

QUESTION 17

LAB 5

You plan to store signed images in an Azure Container Registry instance named az40038443478act1.

You need to modify the SKU for az40038443478aa1 to support the planned images. The solution must minimize costs.

A. See the solution below in explanation

Correct Answer: A

Section:

Explanation:

To store signed images in an Azure Container Registry (ACR) instance and support your planned images while minimizing costs, you need to modify the SKU of your ACR instance to one that supports content trust and image signing. Here's how you can do it:

Determine the Appropriate SKU:

Content trust and image signing are features of the Premium service tier of Azure Container Registry¹.

If cost minimization is a priority, ensure that the Premium tier is necessary for your use case. If you require content trust, the Premium tier is the appropriate choice.

Modify the SKU of the ACR Instance:

Navigate to the Azure Portal.

Go to your ACR instance az40038443478act1.

Select Update from the overview pane.

Choose the Premium SKU from the SKU drop-down menu².

Review the changes and pricing, then save the configuration.

By upgrading to the Premium SKU, you'll be able to store signed images in your ACR instance. Remember to monitor your usage and costs to ensure they align with your budget and requirements.

