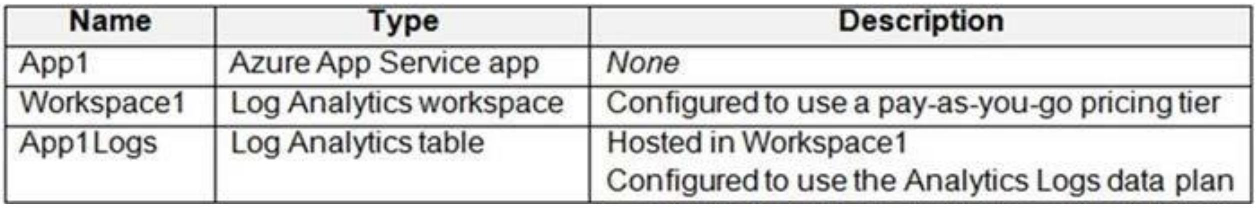
https://www.leads4pass.com/az-305.html

Vendor: Microsoft
Exam Code: AZ-305
Exam Name: Designing Microsoft Azure Infrastructure Solutions
Certification: Microsoft Certifications
Total Questions: 395 Q&A (View Details)
Updated on: Mar 23, 2026

Question 1:

HOTSPOT

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



Name	Type	Description
App1	Azure App Service app	*None*
Workspace1	Log Analytics workspace	Configured to use a pay-as-you-go pricing tier
App1Logs	Log Analytics table	Hosted in Workspace1 Configured to use the Analytics Logs data plan

Log files from App1 are registered to App1Logs. An average of 120 GB of log data is ingested per day.

You configure an Azure Monitor alert that will be triggered if the App1 logs contain error messages.

You need to minimize the Log Analytics costs associated with App1. The solution must meet the following requirements:

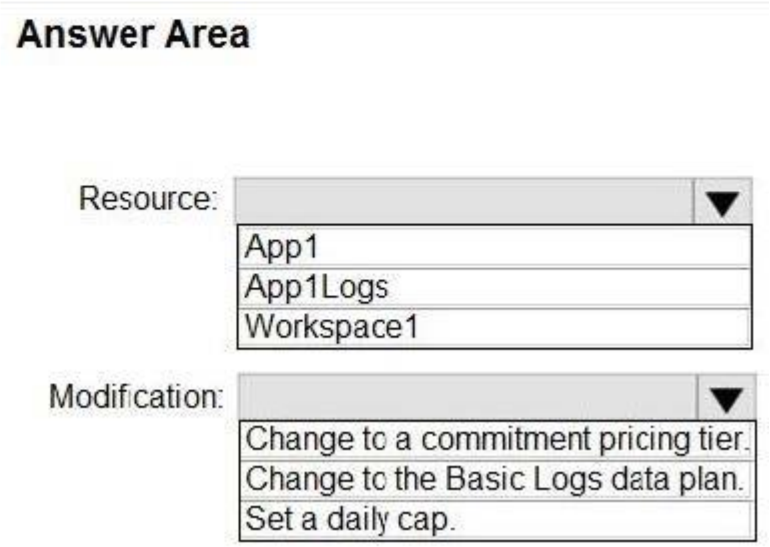
Ensure that all the log files from App1 are ingested to App1Logs.

Minimize the impact on the Azure Monitor alert.

Which resource should you modify, and which modification should you perform? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

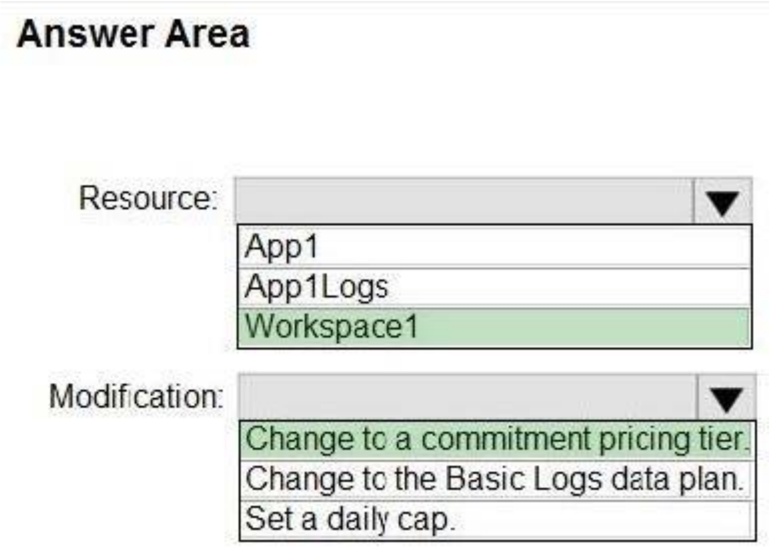
Resource:

- App1
- App1Logs
- Workspace1

Modification:

- Change to a commitment pricing tier.
- Change to the Basic Logs data plan.
- Set a daily cap.

Correct Answer:



Answer Area

Resource:

- App1
- App1Logs
- [✓ Workspace1]

Modification:

- [✓ Change to a commitment pricing tier.]
- Change to the Basic Logs data plan.
- Set a daily cap.

Box 1: Workspace1

Resource

Box 2: Change to a commitment pricing tier

Modification

Commitment tiers

In addition to the pay-as-you-go model, Log Analytics has commitment tiers, which can save you as much as 30 percent compared to the pay-as-you-go price. With commitment tier pricing, you can commit to buy data ingestion for a workspace, starting at 100 GB per day, at a lower price than pay-as-you-go pricing. Any usage above the commitment level (overage) is billed at that same price per GB as provided by the current commitment tier.

Incorrect:

*Change to the Basic Logs data plan.

Would not support alerts.

Note: Azure Monitor Logs offers two log data plans that let you reduce log ingestion and retention costs and take advantage of Azure Monitor\'s advanced features and analytics capabilities based on your needs:

The default Analytics log data plan provides full analysis capabilities and makes log data available for queries, Azure Monitor features, such as alerts, and use by other services.

The Basic log data plan lets you save on the cost of ingesting and storing high-volume verbose logs in your Log Analytics workspace for debugging, troubleshooting, and auditing, but not for analytics and alerts.

* Set a daily cap

A daily cap would not guarantee that all log files are ingested.

Set daily cap on Log Analytics workspace

A daily cap on a Log Analytics workspace allows you to avoid unexpected increases in charges for data ingestion by stopping collection of billable data for the rest of the day whenever a specified threshold is reached.

Reference:
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/cost-logs#commitment-tiers
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/daily-cap
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/basic-logs-configure

Question 2:
DRAG DROP

You have an Azure Synapse instance named AS1 and an Azure Cosmos DB SQL API account named CDB1. CDB1 hosts a container that stores continuously updated operational data.

You plan to use AS1 to analyze the operational data daily.

You need to configure CDB1 to support the analysis by AS1. The solution must meet the following requirements:

1.

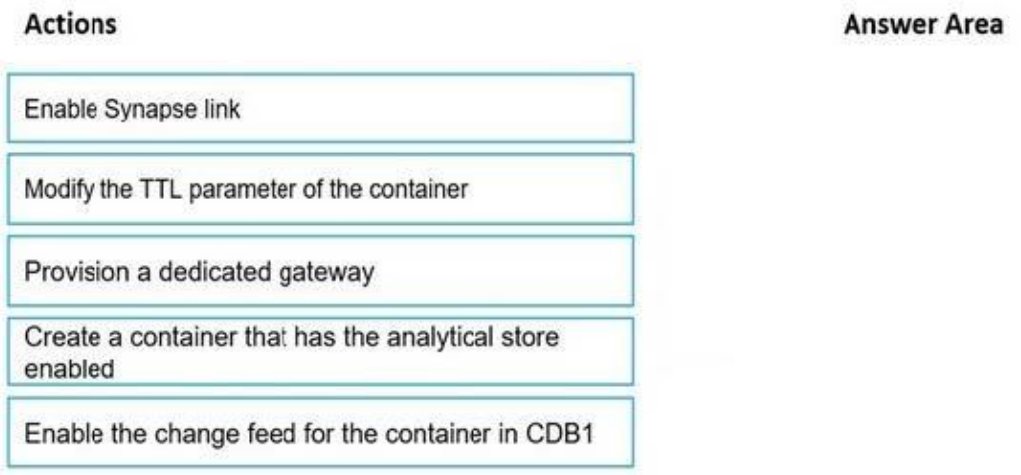
Ensure that AS1 can analyze the operational data without reducing the performance of operations.

2.

Ensure that the analyzed data is deleted automatically.

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

Enable Synapse link

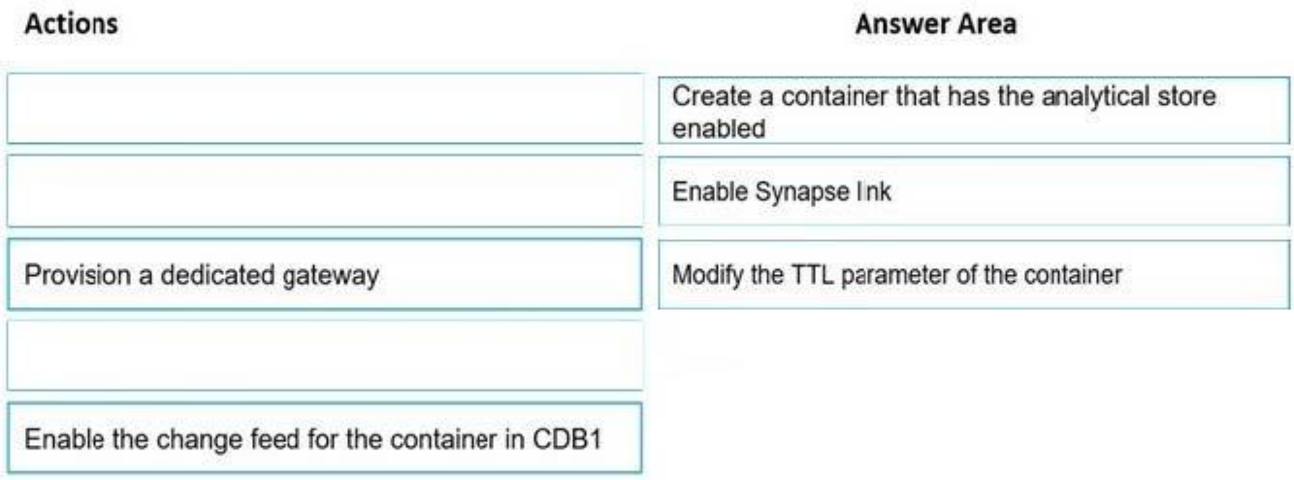
Modify the TTL parameter of the container

Provision a dedicated gateway

Create a container that has the analytical store enabled

Enable the change feed for the container in CDB1

Correct Answer:



Actions

Answer Area

Provision a dedicated gateway

Enable the change feed for the container in CDB1

Create a container that has the analytical store enabled

Enable Synapse lnk

Modify the TTL parameter of the container

Step 1: Create a container that has the analytic store enabled.

Create an analytical store enabled container.

You can turn on analytical store when creating an Azure Cosmos DB container by using one of the following options.

1.

Sign in to the Azure portal or the Azure Cosmos DB Explorer.

2.

Navigate to your Azure Cosmos DB account and open the Data Explorer tab.

3.

Select New Container and enter a name for your database, container, partition key and throughput details. Turn on the Analytical store option.

4.

If you have previously not enabled Synapse Link on this account, it will prompt you to do so because it\'s a pre-requisite to create an analytical store enabled container.

Step 2: Enable Synapse link

Azure Synapse Link allows you to directly access Azure Cosmos DB analytical store using Azure Synapse Analytics without complex data movement. Any updates made to the operational data are visible in the analytical store in near real-

time with no ETL or change feed jobs.

Step 3: Modify the TTL parameter of the container

After you enable the analytical store, it creates a container with analytical TTL property set to the default value of -1 (infinite retention). This setting can be changed later.

Reference:

https://docs.microsoft.com/en-us/azure/cosmos-db/configure-synapse-link

---

Question 3:
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

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

You plan to deploy multiple instances of an Azure web app across several Azure regions.

You need to design an access solution for the app. The solution must meet the following replication requirements:

1.

Support rate limiting.

2.

Balance requests between all instances.

3.

Ensure that users can access the app in the event of a regional outage. Solution: You use Azure Application Gateway to provide access to the app. Does this meet the goal?

A. Yes

B. No

Correct Answer: A

https://learn.microsoft.com/en-us/azure/frontdoor/front-door-overview Azure Front Door is Microsoft\'s modern cloud Content Delivery Network (CDN) that provides fast, reliable, and secure access between your users and your applications' static and dynamic web content across the globe. Azure Front Door delivers your content using the Microsoft\'s global edge network with hundreds of global and local points of presence (PoPs) distributed around the world close to both your enterprise and consumer end users.

Question 4:
Your company develops Azure applications.

You need to recommend a solution for the deployment of Azure subscriptions. The solution must meet the following requirements:

What should you include in the recommendation?

A. Provision resource groups.

B. Support deployments across all Azure regions.

C. Create custom role-based access control (RBAC) roles.

D. Provide consistent virtual machine and virtual network configurations.

Correct Answer: D

Resource groups: You can scope your deployment to a resource group. You use an Azure Resource Manager template (ARM template) for the deployment. Regions: If you have a template spec in one region and want to move it to new

region, you can export the template spec and redeploy it. RBAC: Azure role- based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups,

service principals, or managed identities at a particular scope. In addition to using Azure PowerShell or the Azure CLI, you can assign roles using Azure Resource Manager templates. Templates can be helpful if you need to deploy resources

consistently and repeatedly.

You can setup Virtual machines and virtual network configurations in an Azure Resource Manager template.

Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

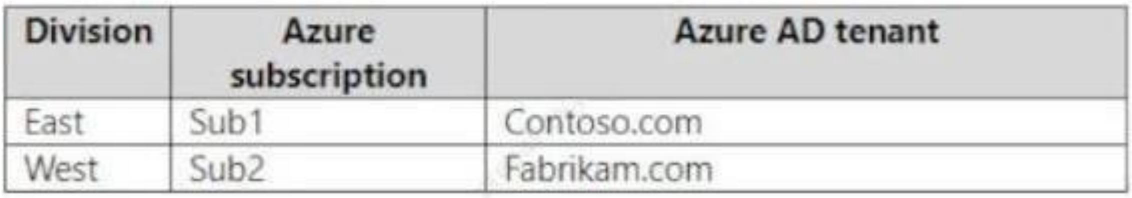
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/microsoft-resources-move-regions

https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-template

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/template-description

Question 5:

Your company has the divisions shown in the following table.



Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

A. Configure Azure AD Identity Protection.

B. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).

C. Configure Supported account types in the application registration and update the sign-in endpoint.

D. Configure a Conditional Access policy.

Correct Answer: C

Identity and account types for single- and multi-tenant apps

You, as a developer, can choose if your app allows only users from your Azure Active Directory (Azure AD) tenant, any Azure AD tenant, or users with personal Microsoft accounts. You can configure your app to be either single tenant or multitenant during app registration in Azure.

Note: A required part of application registration in Azure AD is your selection of supported account types. While IT Pros in administrator roles decide who can consent to apps in their tenant, you, as a developer, specify who can use your app

based on account type. When a tenant doesn\'t allow you to register your application in Azure AD, administrators will provide you with a way to communicate those details to them through another mechanism.

You\'ll choose from the following supported account type options when registering your application.

Accounts in this organizational directory only (O365 only - Single tenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) Personal Microsoft accounts only

Incorrect:

* Configure Azure AD Identity Protection

Identity Protection allows organizations to accomplish three key tasks: Automate the detection and remediation of identity-based risks. Investigate risks using data in the portal. Export risk detection data to other tools.

Reference:

https://learn.microsoft.com/en-us/security/zero-trust/develop/identity-supported-account-types

---

Question 6:
DRAG DROP

You have an Azure Active Directory (Azure AD) tenant. All user accounts are synchronized from an on-premises Active Directory domain and are configured for federated authentication. Active Directory Federation Services (AD FS) servers

are published for external connections by using a farm of Web Application Proxy servers.

You need to recommend a solution to monitor the servers that integrate with Azure AD. The solution must meet the following requirements:

1.

Identify any AD FS issues and their potential resolutions.

2.

Identify any directory synchronization configuration issues and their potential resolutions

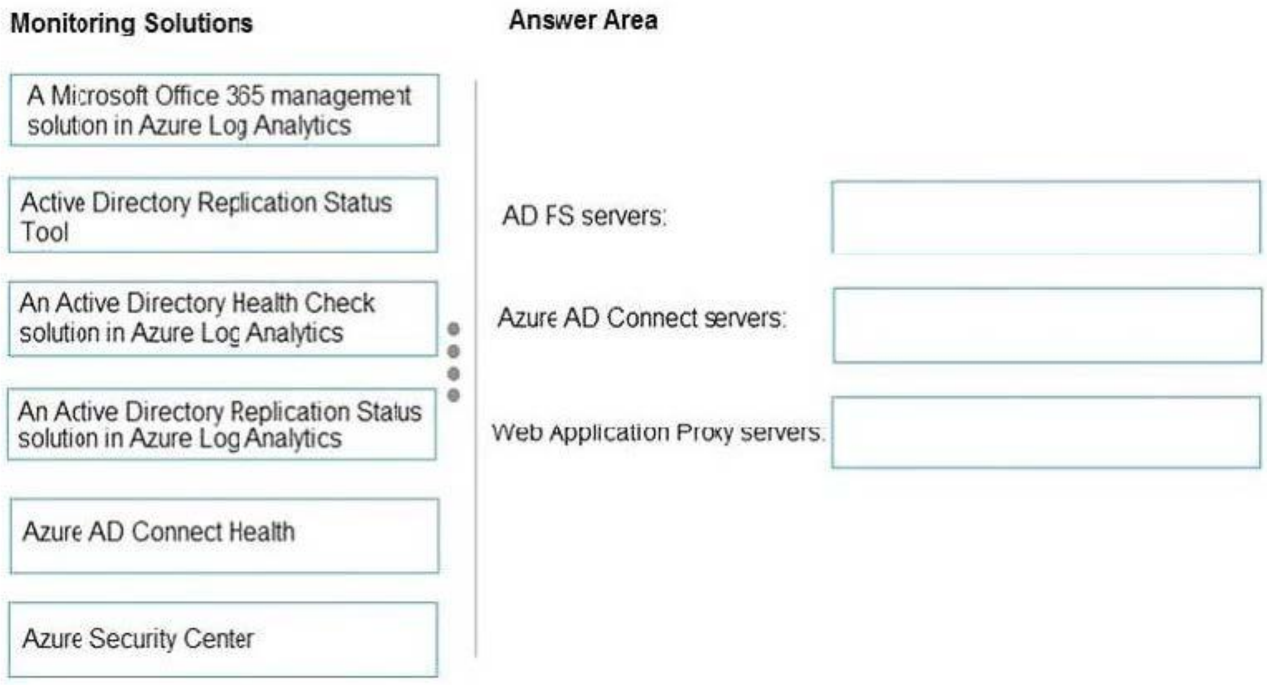
3.

Notify administrators when there are any issues affecting directory synchronization or AD FS operations.

Which monitoring solution should you recommend for each server type?

To answer, drag the appropriate monitoring solutions to the correct server types. Each monitoring solution 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:



Monitoring Solutions

- A Microsoft Office 365 management solution in Azure Log Analytics
- Active Directory Replication Status Tool
- An Active Directory Health Check solution in Azure Log Analytics
- An Active Directory Replication Status solution in Azure Log Analytics
- Azure AD Connect Health
- Azure Security Center

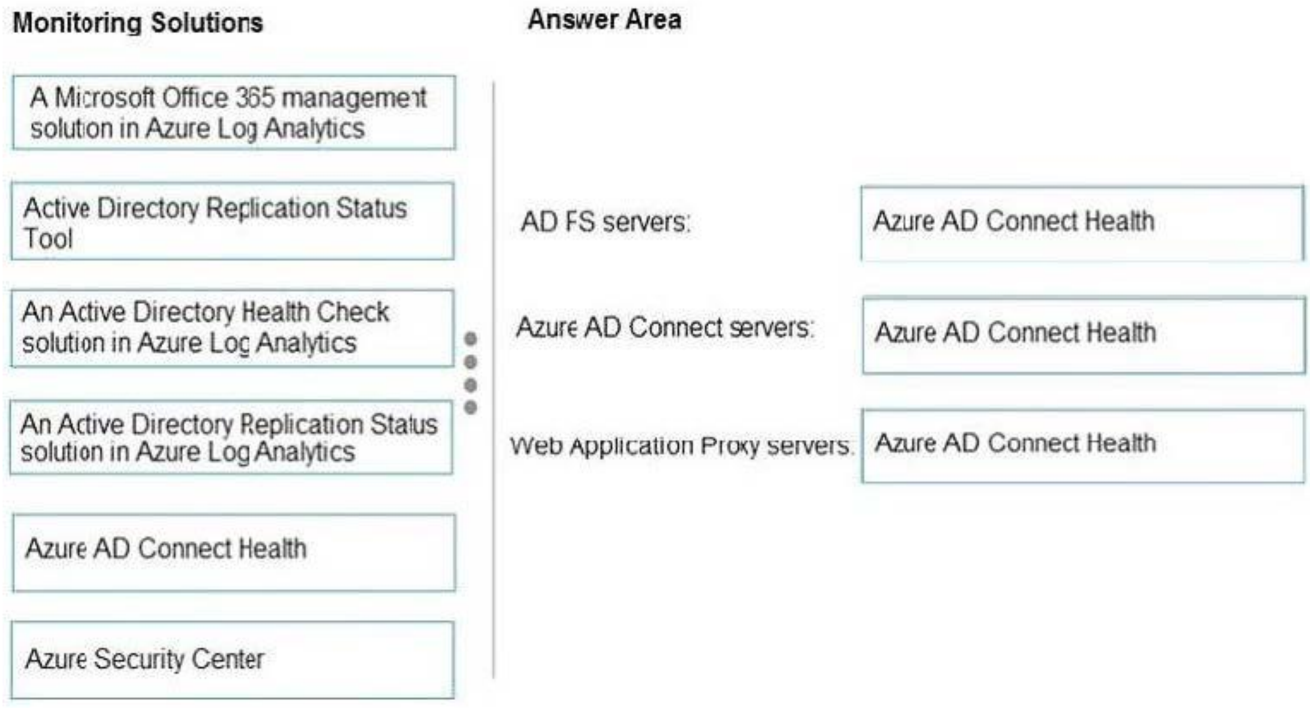
Answer Area

AD FS servers:

Azure AD Connect servers:

Web Application Proxy servers:

Correct Answer:



Monitoring Solutions

A Microsoft Office 365 management solution in Azure Log Analytics

Active Directory Replication Status Tool

An Active Directory Health Check solution in Azure Log Analytics

An Active Directory Replication Status solution in Azure Log Analytics

Azure AD Connect Health

Azure Security Center

Answer Area

AD FS servers:	Azure AD Connect Health
Azure AD Connect servers:	Azure AD Connect Health
Web Application Proxy servers:	Azure AD Connect Health

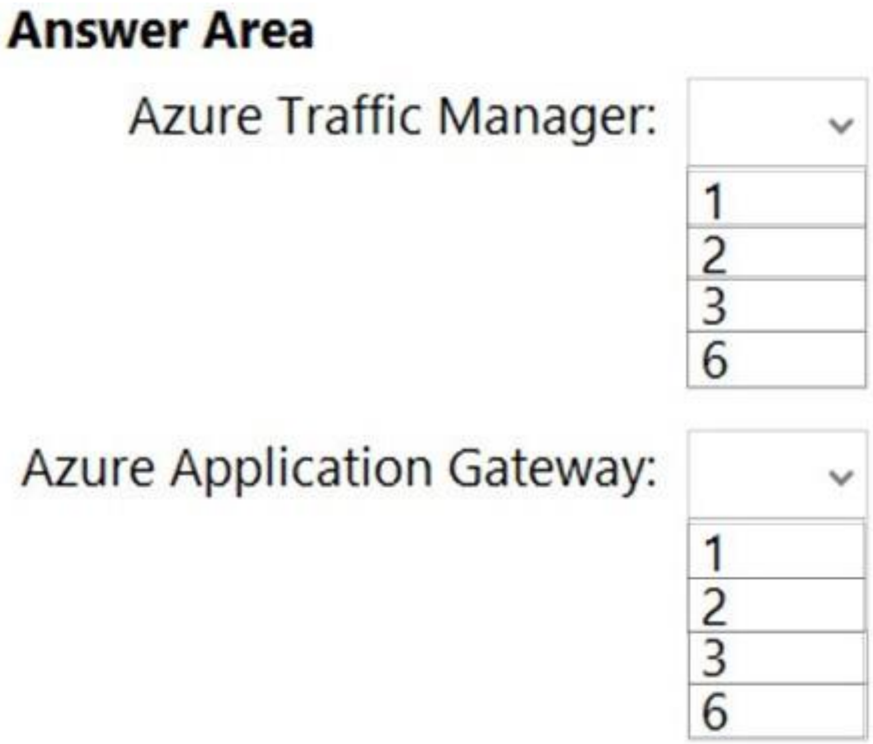
Question 7:
HOTSPOT

You are evaluating whether to use Azure Traffic Manager and Azure Application Gateway to meet the connection requirements for App1.

What is the minimum numbers of instances required for each service? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

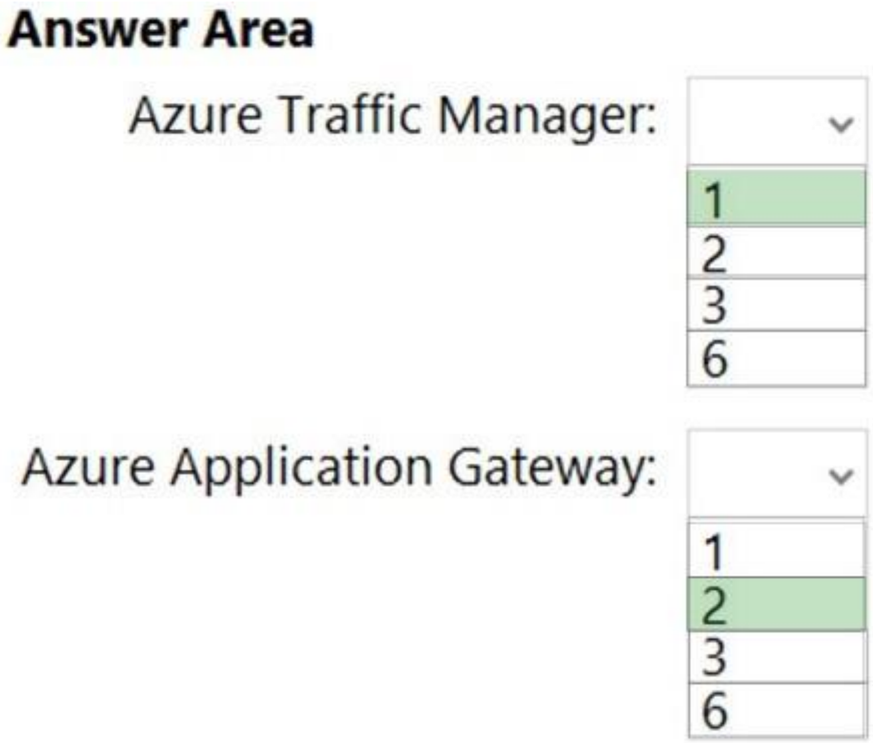
Azure Traffic Manager:

1
2
3
6

Azure Application Gateway:

1
2
3
6

Correct Answer:



Answer Area

Azure Traffic Manager:

[✓ 1]
2
3
6

Azure Application Gateway:

1
[✓ 2]
3
6

Box 1: 1

App1 will only be accessible from the internet. App1 has the following connection requirements:

1.

Connections to App1 must be active-active load balanced between instances.

2.

All connections to App1 from North America must be directed to the East US region.

3.

All other connections must be directed to the West Europe region.

App1 will have six instances: three in the East US Azure region and three in the West Europe Azure region.

Note: Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions.

Box 2: 2

For production workloads, run at least two gateway instances.

A single Application Gateway deployment can run multiple instances of the gateway.

Use one Application Gateway in East US Region, and one in the West Europe region.

Reference:

https://docs.microsoft.com/en-us/azure/architecture/high-availability/reference-architecture-traffic-manager-application-gateway

---

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.

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Install and configure the Microsoft Monitoring Agent and the Dependency Agent on all VMs. Use the Wire Data solution in Azure Monitor to analyze the network traffic.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Note: Wire Data looks at network data at the application level, not down at the TCP transport layer. The solution doesn\'t look at individual ACKs and SYNs.

Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

---

Question 9:
HOTSPOT

You plan to deploy a containerized web-app that will be hosted in five Azure Kubernetes Service (AKS) clusters. Each cluster will be hosted in a different Azure region.

You need to provide access to the app from the internet. The solution must meet the following requirements:

1.

Incoming HTTPS requests must be routed to the cluster that has the lowest network latency.

2.

HTTPS traffic to individual pods must be routed via an ingress controller.

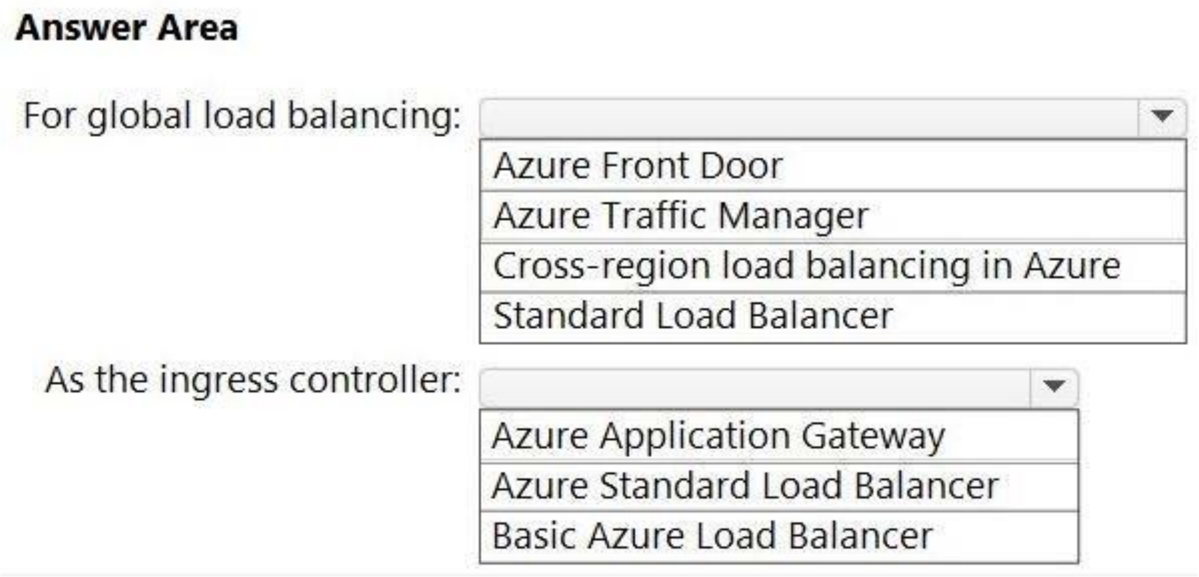
3.

In the event of an AKS cluster outage, failover time must be minimized.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

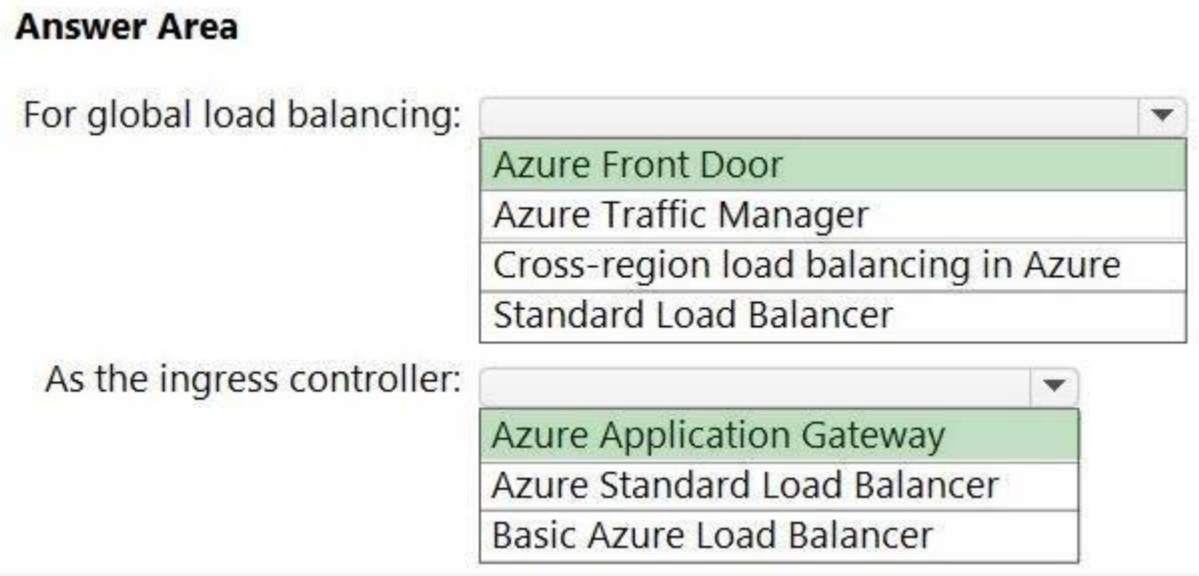
For global load balancing:

- Azure Front Door
- Azure Traffic Manager
- Cross-region load balancing in Azure
- Standard Load Balancer

As the ingress controller:

- Azure Application Gateway
- Azure Standard Load Balancer
- Basic Azure Load Balancer

Correct Answer:



Answer Area

For global load balancing:

- [✓ Azure Front Door]
- Azure Traffic Manager
- Cross-region load balancing in Azure
- Standard Load Balancer

As the ingress controller:

- [✓ Azure Application Gateway]
- Azure Standard Load Balancer
- Basic Azure Load Balancer

Reference:
https://learn.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview
https://learn.microsoft.com/en-us/azure/application-gateway/ingress-controller-overview

https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq

Question 10:
HOTSPOT

You have an Azure subscription that contains an Azure key vault named KV1 and a virtual machine named VM1. VM1 runs Windows Server 2022: Azure Edition.

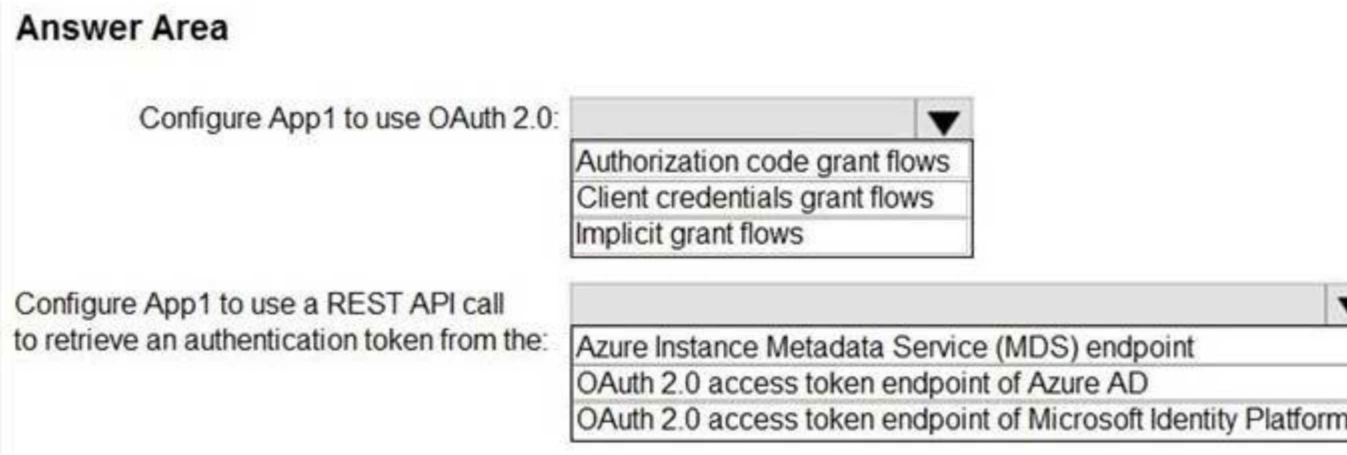
You plan to deploy an ASP.Net Core-based application named App1 to VM1.

You need to configure App1 to use a system-assigned managed identity to retrieve secrets from KV1. The solution must minimize development effort.

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

NOTE: Each correct selection is worth one point.

Hot Area:

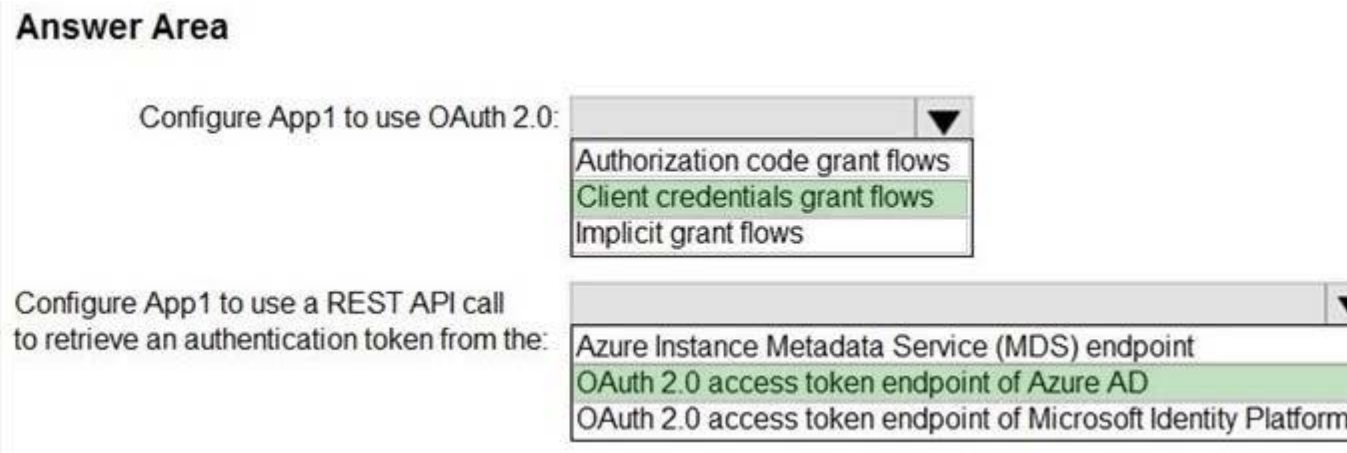


Answer Area

Configure App1 to use OAuth 2.0:
- Authorization code grant flows
- Client credentials grant flows
- Implicit grant flows

Configure App1 to use a REST API call to retrieve an authentication token from the:
- Azure Instance Metadata Service (MDS) endpoint
- OAuth 2.0 access token endpoint of Azure AD
- OAuth 2.0 access token endpoint of Microsoft Identity Platform

Correct Answer:



Answer Area

Configure App1 to use OAuth 2.0:
- Authorization code grant flows
- [✓ Client credentials grant flows]
- Implicit grant flows

Configure App1 to use a REST API call to retrieve an authentication token from the:
- Azure Instance Metadata Service (MDS) endpoint
- [✓ OAuth 2.0 access token endpoint of Azure AD]
- OAuth 2.0 access token endpoint of Microsoft Identity Platform

Box 1: Client Credentials flow Client Credentials flow - The only flow that does not require immediate user interaction, usually used when the OAuth client is acting on-behalf of itself, when user-consent doesn\'t make sense, or when authorization primitives could be configured out-of-band (for instance via Azure AD)

Note: Authenticating to Azure Services Local machines don\'t support managed identities for Azure resources. As a result, the Microsoft.Azure.Services.AppAuthentication library uses your developer credentials to run in your local development environment. When the solution is deployed to Azure, the library uses a managed identity to switch to an OAuth 2.0

client credential grant flow. This approach means you can test the same code locally and remotely without worry.

Incorrect:

*

Authorization code flow - Requires user interaction and consent, typically via the web browser, to get a code which is then used to issue an access token.

*

Implicit grant flow - Created for single page web / mobile webview apps, where token creation and handling is done entirely from the front end.

Box 2: OAuth 2.0 access token endpoint of Azure AD

Example: Issuing and inspecting our first OAuth token

At this stage, we should be able to issue tokens to Service A, on behalf of Service B - let\'s see that in action.

In Azure AD application registration blade, go to Service B (as shown in previous steps)

In the Overview blade, Click on the ‘Endpoints

Question 11:

You have an Azure subscription that contains an Azure Blob storage account named store1.

You have an on-premises file server named Server1 that runs Windows Server 2016. Server1 stores 500 GB of company files.

You need to store a copy of the company files from Server 1 in store1.

Which two possible Azure services achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. an integration account

B. an On-premises data gateway

C. an Azure Batch account

D. an Azure Import/Export job

E. Azure Data Factory

Correct Answer: DE

Question 12:
You need to deploy resources to host a stateless web app in an Azure subscription. The solution must meet the following requirements:

1.

Provide access to the full .NET framework.

2.

Provide redundancy if an Azure region fails.

3.

Grant administrators access to the operating system to install custom application dependencies.

Solution: You deploy an Azure virtual machine scale set that uses autoscaling.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead, you should deploy two Azure virtual machines to two Azure regions, and you create a Traffic Manager profile

Question 13:
You are designing a microservices architecture that will support a web application. The solution must meet the following requirements:

1.

Allow independent upgrades to each microservice

2.

Deploy the solution on-premises and to Azure Set policies for performing automatic repairs to the microservices Support low-latency and hyper-scale operations You need to recommend a technology. What should you recommend?

A. Azure Service Fabric

B. Azure Container Service

C. Azure Container Instance

D. Azure Virtual Machine Scale Set

Correct Answer: A

https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-overview

Question 14:
HOTSPOT

Your company has 20 web APIs that were developed in-house.

The company is developing 10 web apps that will use the web APIs. The web apps and the APIs are registered in the company s Azure AD tenant. The web APIs are published by using Azure API Management.

You need to recommend a solution to block unauthorized requests originating from the web apps from reaching the web APIs. The solution must meet the following requirements:

1.

Use Azure AD-generated claims.

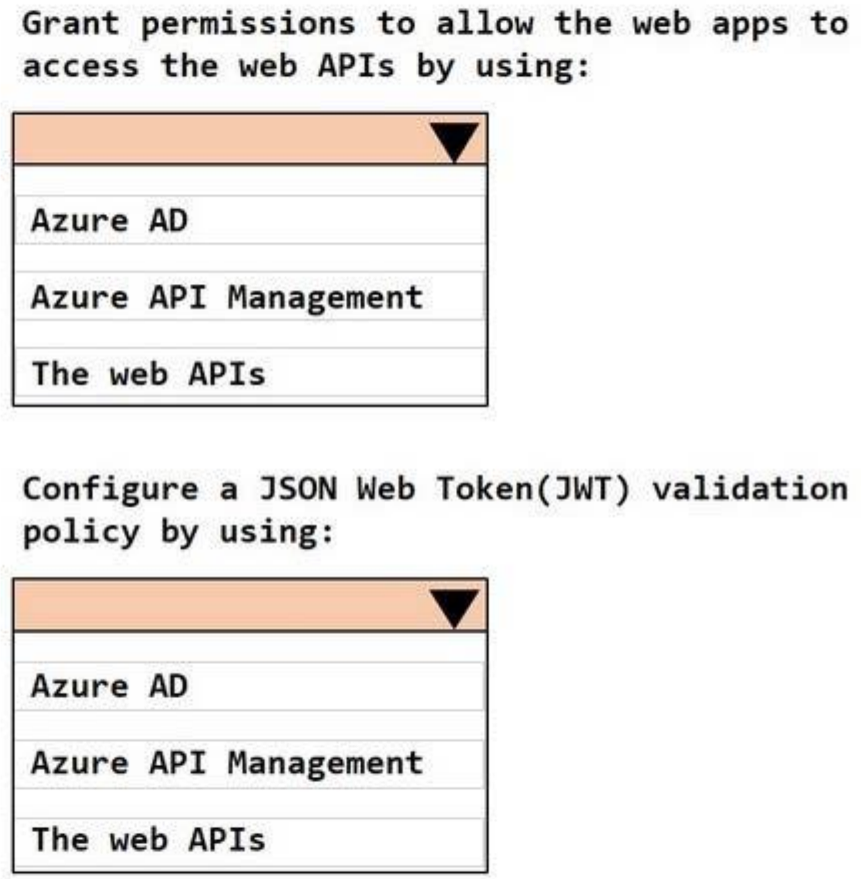
2.

Minimize configuration and management effort

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

NOTE: Each correct selection is worth one point.

Hot Area:



Grant permissions to allow the web apps to access the web APIs by using:

▼

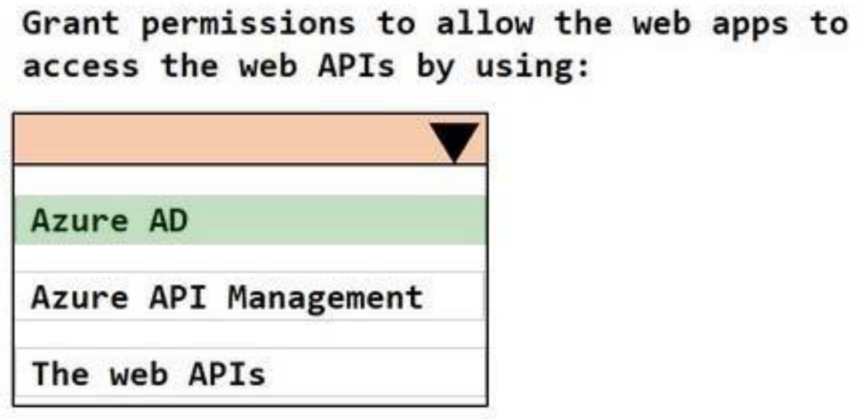
- Azure AD
- Azure API Management
- The web APIs

Configure a JSON Web Token(JWT) validation policy by using:

▼

- Azure AD
- Azure API Management
- The web APIs

Correct Answer:

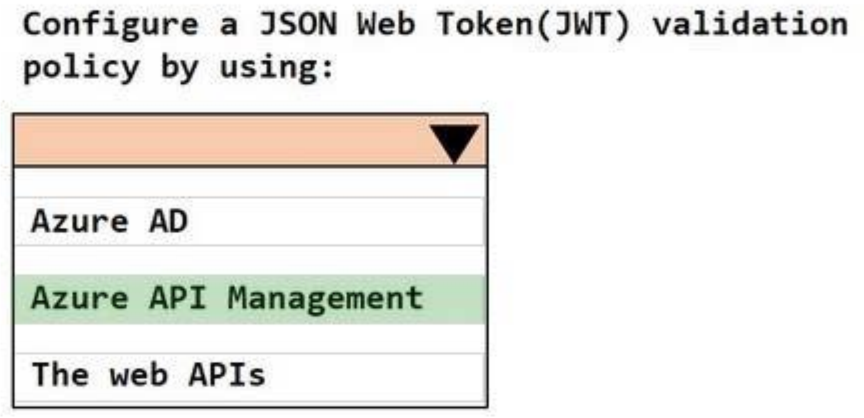


Grant permissions to allow the web apps to access the web APIs by using:

[✓ Azure AD]

Azure API Management

The web APIs



Configure a JSON Web Token(JWT) validation policy by using:

Azure AD

[✓ Azure API Management]

The web APIs

Question 15:
You create an Azure Kubernetes Service (AKS) duster and an Azure Container Registry.

You need to perform continuous deployments of a containerized application to the AKS cluster as soon as the image updates in the registry.

What should you use to perform the deployments?

A. an Azure Pipelines release pipeline

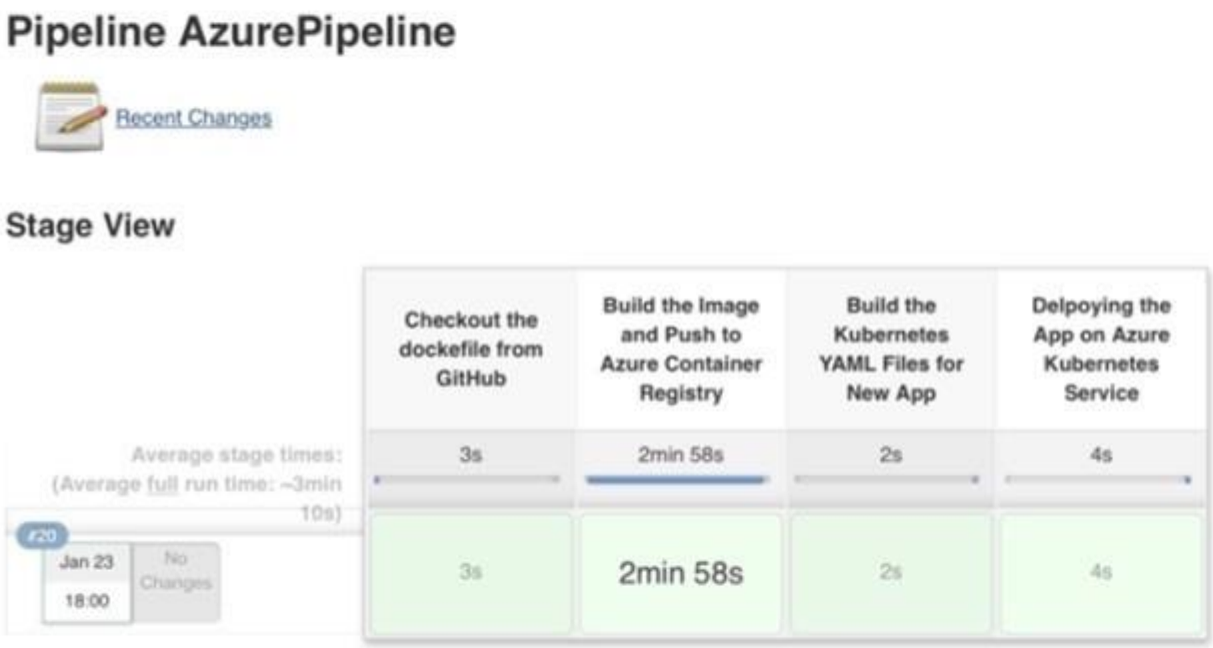
B. an Azure Automation runbook

C. an Azure Resource Manager template

D. a kubectl script from a CRON job

Correct Answer: A

You can implement a Continuous Deployment pipeline. Example:



Pipeline AzurePipeline

Recent Changes

Stage View

	Checkout the dockefile from GitHub	Build the Image and Push to Azure Container Registry	Build the Kubernetes YAML Files for New App	Delpoying the App on Azure Kubernetes Service
Average stage times: (Average full run time: ~3min 10s)	3s	2min 58s	2s	4s
#20 Jan 23 18:00 No Changes	3s	2min 58s	2s	4s

What the pipeline accomplishes :

Stage 1: The code gets pushed in the Github. The Jenkins job gets triggered automatically.

The Dockerfile is checked out from Github.

Stage 2: Docker builds an image from the Dockerfile and then the image is tagged with the build number. Additionally, the latest tag is also attached to the image for the containers to use. Stage 3: We have default deployment and service

YAML files stored on the Jenkins server. Jenkins makes a copy of the default YAML files, make the necessary changes according to the build and put them in a separate folder.

Stage 4: kubectl was initially configured at the time of setting up AKS on the Jenkins server. The YAML files are fed to the kubectl util which in turn creates pods and services.

Reference:

https://medium.com/velotio-perspectives/continuous-deployment-with-azure-kubernetes-service-azure-container-registry-jenkins-ca337940151b