AZ-204^Q&As

Developing Solutions for Microsoft Azure

QUESTION 1

You are building an application to track cell towers that are available to phones in near real time. A phone will send information to the application by using the Azure Web PubSub service. The data will be processed by using an Azure

Functions app. Traffic will be transmitted by using a content delivery network (CDN).

The Azure function must be protected against misconfigured or unauthorized invocations.

You need to ensure that the CDN allows for the Azure function protection.

Which HTTP header should be on the allowed list?

A. Authorization

B. WebHook-Request-Callback

C. Resource

D. WebHook-Request-Origin

Correct Answer: D

CloudEvents extension for Azure Web PubSub event handler with HTTP protocol

The Web PubSub service delivers client events to the upstream webhook using the CloudEvents HTTP protocol binding.

Webhook validation

The Webhook validation follows CloudEvents. The request always contains WebHook-Request-Origin: xxx.webpubsub.azure.com in the header.

If and only if the delivery target does allow delivery of the events, it MUST reply to the request by including WebHook-Allowed-Origin header, for example:

WebHook-Allowed-Origin: *

Or:

WebHook-Allowed-Origin: xxx.webpubsub.azure.com

For now, WebHook-Request-Rate and WebHook-Request-Callback are not supported.

Incorrect:

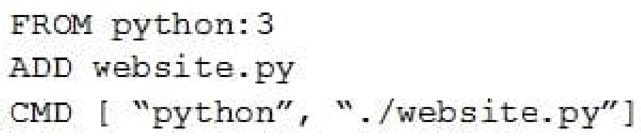
* WebHook-Request-Callback. An optional field that provides the webhook with an alternative to grant permission asynchronously, by way of a HTTP callback.

Reference: https://learn.microsoft.com/en-us/azure/azure-web-pubsub/reference-cloud-events

QUESTION 2

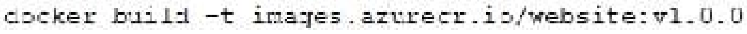
HOTSPOT

You are preparing to deploy a Python website to an Azure Web App using a container. The solution will use multiple containers in the same container group. The Dockerfile that builds the container is as follows:



```
FROM python:3
ADD website.py
CMD [ "python", "./website.py"]
```

You build a container by using the following command. The Azure Container Registry instance named images is a private registry.



```
docker build -t images.azurecr.io/website:v1.0.0
```

The user name and password for the registry is admin.

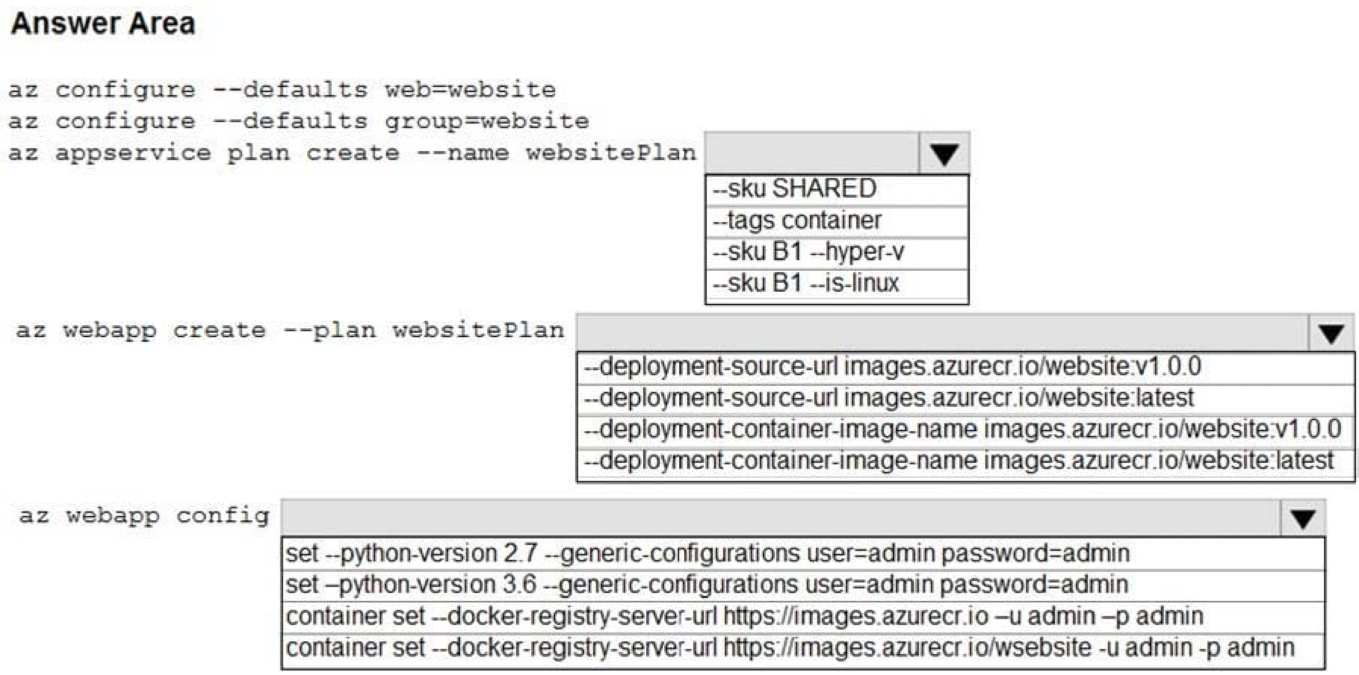
The Web App must always run the same version of the website regardless of future builds.

You need to create an Azure Web App to run the website.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

```
az configure --defaults web=website
az configure --defaults group=website
az appservice plan create --name websitePlan
```

- --sku SHARED
- --tags container
- --sku B1 --hyper-v
- --sku B1 --is-linux

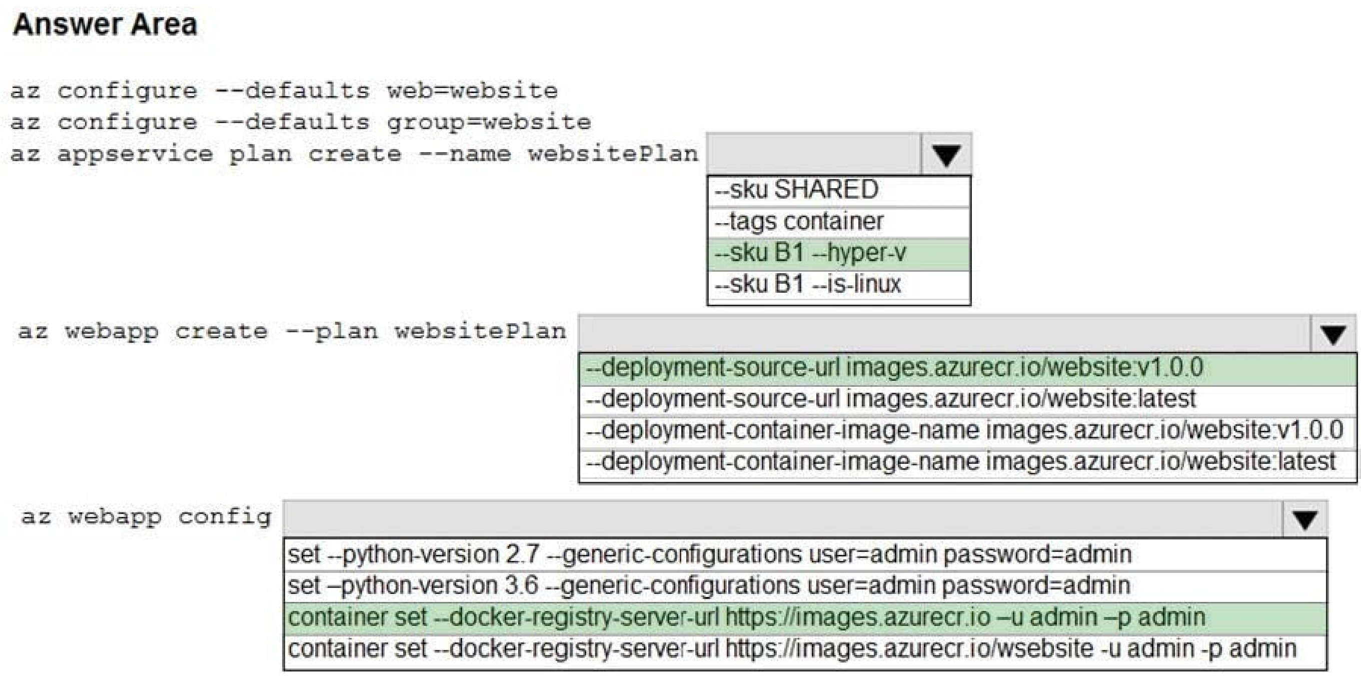
```
az webapp create --plan websitePlan
```

- --deployment-source-url images.azurecr.io/website:v1.0.0
- --deployment-source-url images.azurecr.io/website:latest
- --deployment-container-image-name images.azurecr.io/website:v1.0.0
- --deployment-container-image-name images.azurecr.io/website:latest

```
az webapp config
```

- set --python-version 2.7 --generic-configurations user=admin password=admin
- set –python-version 3.6 --generic-configurations user=admin password=admin
- container set --docker-registry-server-url https://images.azurecr.io –u admin –p admin
- container set --docker-registry-server-url https://images.azurecr.io/wsebsite -u admin -p admin

Correct Answer:



Answer Area

```
az configure --defaults web=website
az configure --defaults group=website
az appservice plan create --name websitePlan
```

--sku SHARED
--tags container
--sku B1 --hyper-v
--sku B1 --is-linux

```
az webapp create --plan websitePlan
```

--deployment-source-url images.azurecr.io/website:v1.0.0
--deployment-source-url images.azurecr.io/website:latest
--deployment-container-image-name images.azurecr.io/website:v1.0.0
--deployment-container-image-name images.azurecr.io/website:latest

```
az webapp config
```

set --python-version 2.7 --generic-configurations user=admin password=admin
set –python-version 3.6 --generic-configurations user=admin password=admin
container set --docker-registry-server-url https://images.azurecr.io –u admin –p admin
container set --docker-registry-server-url https://images.azurecr.io/wsebsite -u admin -p admin

Box 1: --SKU B1 --hyper-v

--hyper-v

Host web app on Windows container.

Box 2: --deployment-source-url images.azurecr.io/website:v1.0.0

--deployment-source-url -u

Git repository URL to link with manual integration.

The Web App must always run the same version of the website regardless of future builds.

Incorrect:

--deployment-container-image-name -i

Linux only. Container image name from Docker Hub, e.g. publisher/image-name:tag.

Box 3: az webapp config container set -url https://images.azurecr.io -u admin -p admin

az webapp config container set

Set a web app container\\'s settings.

Paremeter: --docker-registry-server-url -r

The container registry server url.

The Azure Container Registry instance named images is a private registry.

Example:

az webapp config container set --docker-registry-server-url https://{azure-container-registry-name}.azurecr.io

Reference:

https://docs.microsoft.com/en-us/cli/azure/appservice/plan

QUESTION 3

Your company\\'s Azure subscription includes an Azure Log Analytics workspace.

Your company has a hundred on-premises servers that run either Windows Server 2012 R2 or Windows Server 2016, and is linked to the Azure Log Analytics workspace. The Azure Log Analytics workspace is set up to gather performance

counters associated with security from these linked servers.

You must configure alerts based on the information gathered by the Azure Log Analytics workspace.

You have to make sure that alert rules allow for dimensions, and that alert creation time should be kept to a minimum. Furthermore, a single alert notification must be created when the alert is created and when the alert is resolved.

You need to make use of the necessary signal type when creating the alert rules.

Which of the following is the option you should use?

A. The Activity log signal type.

B. The Application Log signal type.

C. The Metric signal type.

D. The Audit Log signal type.

Correct Answer: C

Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.

Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.

Reference:

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

QUESTION 4

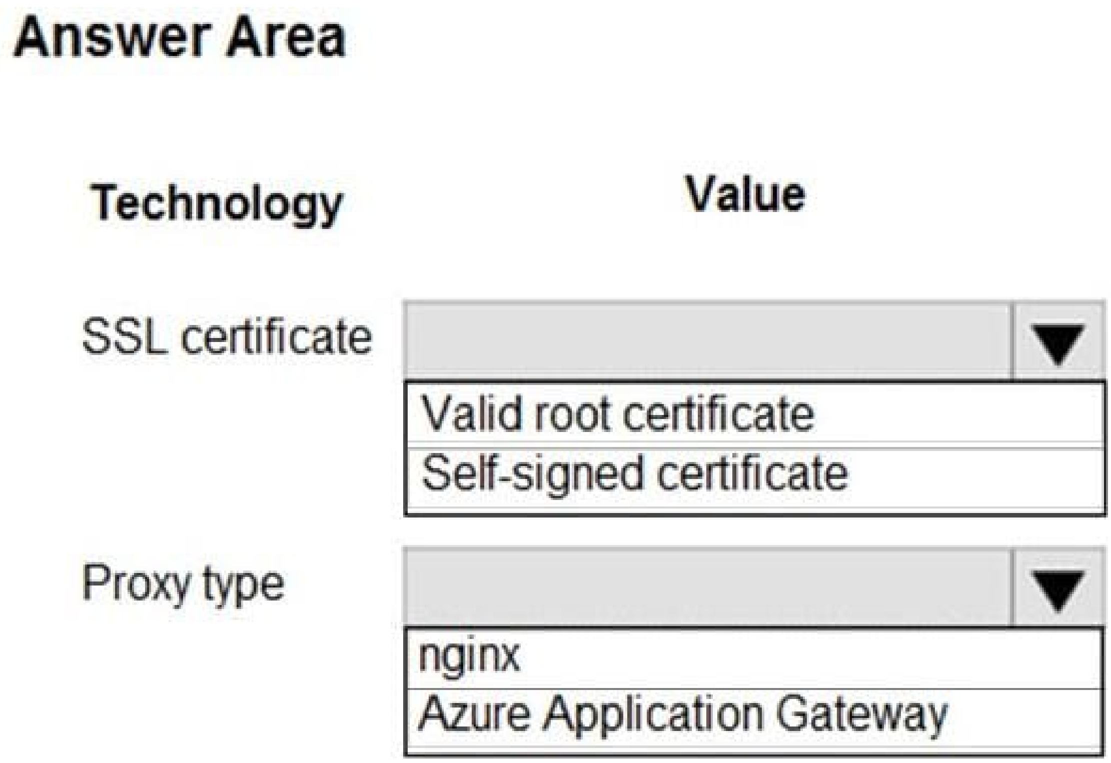
HOTSPOT

You need to ensure that network security policies are met.

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

NOTE: Each correct selection is worth one point.

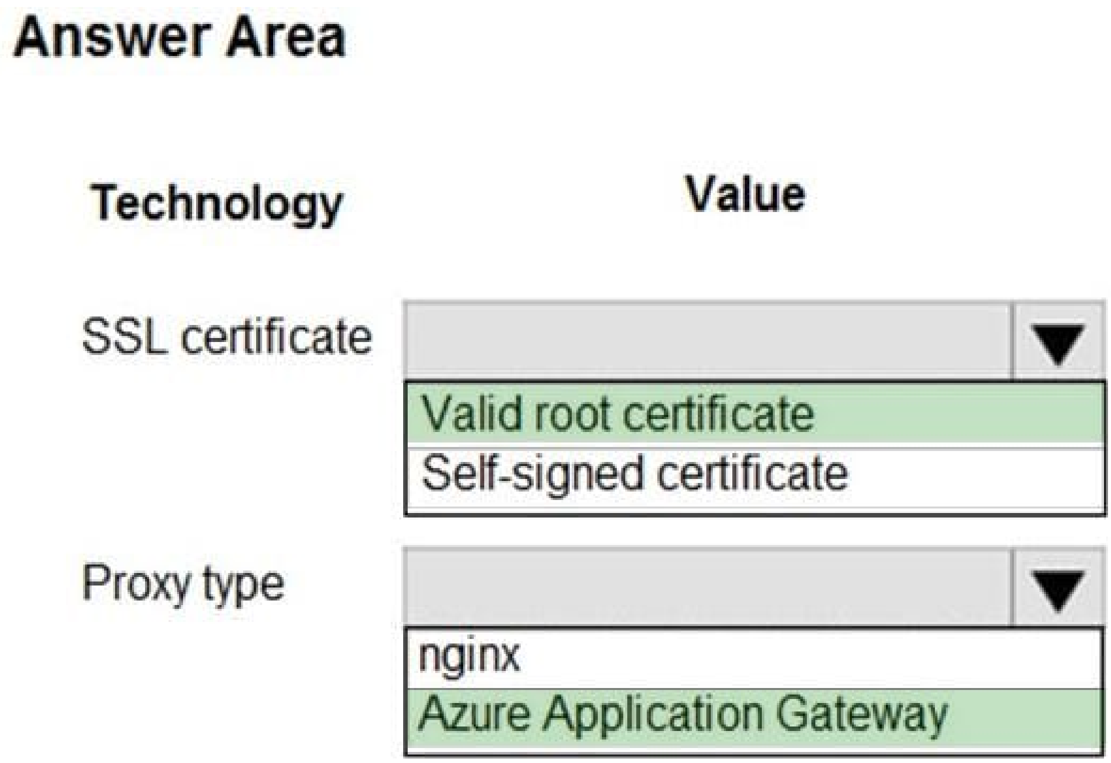
Hot Area:



Answer Area

Technology	Value
SSL certificate	Valid root certificate Self-signed certificate
Proxy type	nginx Azure Application Gateway

Correct Answer:



Answer Area

Technology	Value
SSL certificate	[✓ Valid root certificate] Self-signed certificate
Proxy type	nginx [✓ Azure Application Gateway]

Box 1: Valid root certificate

Scenario: All websites and services must use SSL from a valid root certificate authority.

Box 2: Azure Application Gateway

Scenario:

Any web service accessible over the Internet must be protected from cross site scripting attacks.

All Internal services must only be accessible from Internal Virtual Networks (VNets)

All parts of the system must support inbound and outbound traffic restrictions.

Azure Web Application Firewall (WAF) on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that

exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

Application Gateway supports autoscaling, SSL offloading, and end-to-end SSL, a web application firewall (WAF), cookie-based session affinity, URL path-based routing, multisite hosting, redirection, rewrite HTTP headers and other features.

Note: Both Nginx and Azure Application Gateway act as a reverse proxy with Layer 7 load-balancing features plus a WAF to ensure strong protection against common web vulnerabilities and exploits.

You can modify Nginx web server configuration/SSL for X-XSS protection. This helps to prevent cross-site scripting exploits by forcing the injection of HTTP headers with X-XSS protection.

Reference:

https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview

https://www.upguard.com/articles/10-tips-for-securing-your-nginx-deployment

QUESTION 5

You a web application that provides access to legal documents that are stored on Azure Blob Storage with version level immutability policies. Documents are protected with both time-based policies legal hold policies. All time--based retention

policies have Allow Protected Append Writes property enabled.

You have a requirement to prevent the user from attempting to perform operations that would fail only a legal is in effect and when all other are expired

You reed to meet the requirement.

Which two operations you prevent?

A. adding data to documents

B. deleting documents

C. creating documents

D. overwriting existing documents

Correct Answer: BD

The Append Block operation is permitted only for policies with the allowProtectedAppendWrites or allowProtectedAppendWritesAll property enabled.

The AllowProtectedAppendWrites property setting allows for writing new blocks to an append blob while maintaining immutability protection and compliance. If this setting is enabled, you can create an append blob directly in the policy-protected container, and then continue to add new blocks of data to the end of the append blob with the Append Block operation. Only new blocks can be added; any existing blocks can\\'t be modified or deleted. Enabling this setting doesn\\'t affect the immutability behavior of block blobs or page blobs.

Reference: https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-time-based-retention-policy-overview#allow-protected-append-blobs-writes