

- **Vendor: Microsoft**
- **Exam Code: AZ-204**
- **Exam Name: Developing Solutions for Microsoft Azure**
- **New Updated Questions from [Braindump2go](https://www.braindump2go.com) (Updated in [Nov./2020](#))**

Visit Braindump2go and Download Full Version AZ-204 Exam Dumps

QUESTION 67

Case Study 3 - City Power & Light

Background

City Power & Light company provides electrical infrastructure monitoring solutions for homes and businesses. The company is migrating solutions to Azure.

Current environment

Architecture overview

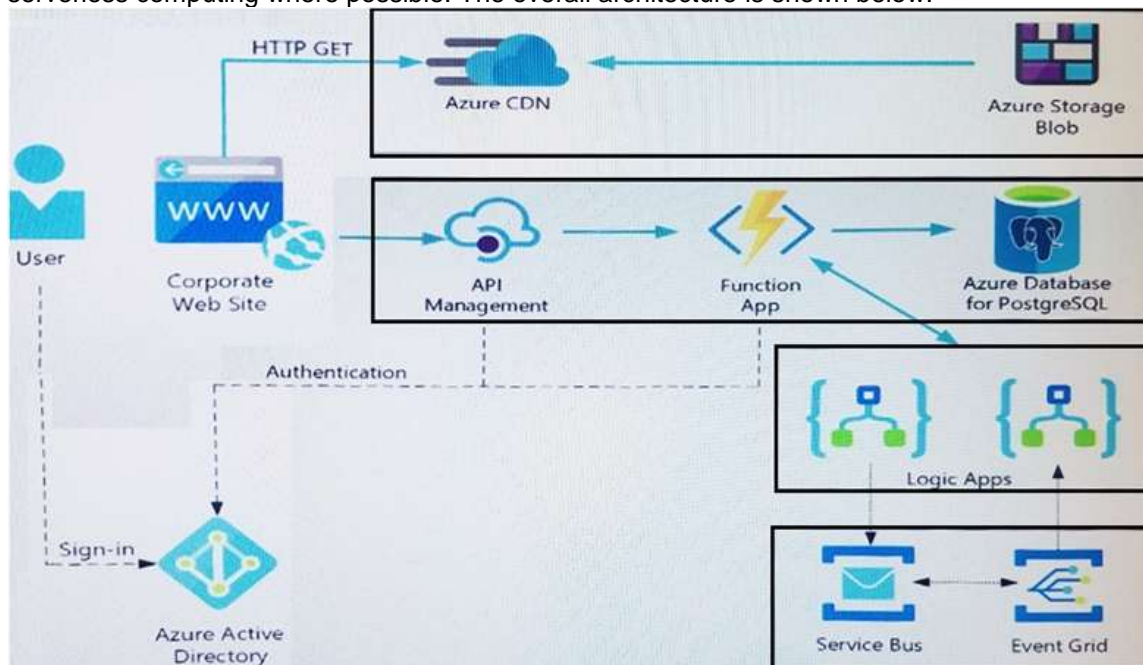
The company has a public website located at <http://www.cpandl.com/>. The site is a single-page web application that runs in Azure App Service on Linux. The website uses files stored in Azure Storage and cached in Azure Content Delivery Network (CDN) to serve static content.

API Management and Azure Function App functions are used to process and store data in Azure Database for PostgreSQL. API Management is used to broker communications to the Azure Function app functions for Logic app integration. Logic apps are used to orchestrate the data processing while Service Bus and Event Grid handle messaging and events.

The solution uses Application Insights, Azure Monitor, and Azure Key Vault.

Architecture diagram

The company has several applications and services that support their business. The company plans to implement serverless computing where possible. The overall architecture is shown below.



User authentication

The following steps detail the user authentication process:

1. The user selects **Sign in** in the website.
2. The browser redirects the user to the Azure Active Directory (Azure AD) sign in page.
3. The user signs in.
4. Azure AD redirects the user's session back to the web application. The URL includes an access token.

[AZ-204 Exam Dumps](#) [AZ-204 Exam Questions](#) [AZ-204 PDF Dumps](#) [AZ-204 VCE Dumps](#)

<https://www.braindump2go.com/az-204.html>

5. The web application calls an API and includes the access token in the authentication header. The application ID is sent as the audience ('aud') claim in the access token.
6. The back-end API validates the access token.

Requirements**Corporate website**

- Communications and content must be secured by using SSL.
- Communications must use HTTPS.
- Data must be replicated to a secondary region and three availability zones.
- Data storage costs must be minimized.

Azure Database for PostgreSQL

The database connection string is stored in Azure Key Vault with the following attributes:

- Azure Key Vault name: cpandlkeyvault
- Secret name: PostgreSQLConn
- Id: 80df3e46ffcd4f1cb187f79905e9a1e8

The connection information is updated frequently. The application must always use the latest information to connect to the database.

Azure Service Bus and Azure Event Grid

- Azure Event Grid must use Azure Service Bus for queue-based load leveling.
- Events in Azure Event Grid must be routed directly to Service Bus queues for use in buffering.
- Events from Azure Service Bus and other Azure services must continue to be routed to Azure Event Grid for processing.

Security

- All SSL certificates and credentials must be stored in Azure Key Vault.
- File access must restrict access by IP, protocol, and Azure AD rights.
- All user accounts and processes must receive only those privileges which are essential to perform their intended function.

Compliance

Auditing of the file updates and transfers must be enabled to comply with General Data Protection Regulation (GDPR). The file updates must be read-only, stored in the order in which they occurred, include only create, update, delete, and copy operations, and be retained for compliance reasons.

Issues**Corporate website**

While testing the site, the following error message displays:

CryptographicException: The system cannot find the file specified.

Function app

You perform local testing for the RequestUserApproval function. The following error message displays:

'Timeout value of 00:10:00 exceeded by function: RequestUserApproval'

The same error message displays when you test the function in an Azure development environment when you run the following Kusto query:

```
FunctionAppLogs  
| where FunctionName == "RequestUserApproval"
```

Logic app

You test the Logic app in a development environment. The following error message displays:

'400 Bad Request'

Troubleshooting of the error shows an HttpTrigger action to call the RequestUserApproval function.

Code**Corporate website**

Security.cs:

```
SC01 public class Security  
SC02 {  
SC03 var bytes = System.IO.File.ReadAllBytes("~/var/ssl/private");  
SC04 var cert = new System.Security.Cryptography.X509Certificate2(bytes);  
SC05 var certName = cert.FriendlyName;  
SC06 }
```

Function app

RequestUserApproval.cs:

```
RA01 public static class RequestUserApproval
RA02 {
RA03 [FunctionName("RequestUserApproval")]
RA04 public static async Task<ActionResult> Run(
RA05 [HttpTrigger(AuthorizationLevel.Function, "get", "post", Route = null)] HttpRequest req,
RA06 ILogger log)
RA07 {
RA08     log.LogInformation("RequestUserApproval function processed a request.");
RA09     return ProcessRequest(req)
RA10     ? (ActionResult)new OkObjectResult($"User approval processed")
RA11     : new BadRequestObjectResult("Failed to process user approval");
RA12 }
RA13 private static bool ProcessRequest(HttpRequest req)
RA14 {
RA15     ...
RA16 }
RA17 }
```

You need to correct the RequestUserApproval Function app error.
What should you do?

- A. Update line RA13 to use the async keyword and return an HttpRequest object value.
- B. Configure the Function app to use an App Service hosting plan. Enable the Always On setting of the hosting plan.
- C. Update the function to be stateful by using Durable Functions to process the request payload.
- D. Update the functionTimeout property of the host.json project file to 15 minutes.

Answer: C

Explanation:

Async operation tracking

The HTTP response mentioned previously is designed to help implement long-running HTTP async APIs with Durable Functions. This pattern is sometimes referred to as the polling consumer pattern.

Both the client and server implementations of this pattern are built into the Durable Functions HTTP APIs.

Function app

You perform local testing for the RequestUserApproval function. The following error message displays:

'Timeout value of 00:10:00 exceeded by function: RequestUserApproval' The same error message displays when you test the function in an Azure development environment when you run the following Kusto query:

FunctionAppLogs

| where FunctionName == "RequestUserApproval"

References:

<https://docs.microsoft.com/en-us/azure/azure-functions/durable/durable-functions-http-features>

QUESTION 68

Case Study 3 - City Power & Light

Background

City Power & Light company provides electrical infrastructure monitoring solutions for homes and businesses. The company is migrating solutions to Azure.

Current environment

Architecture overview

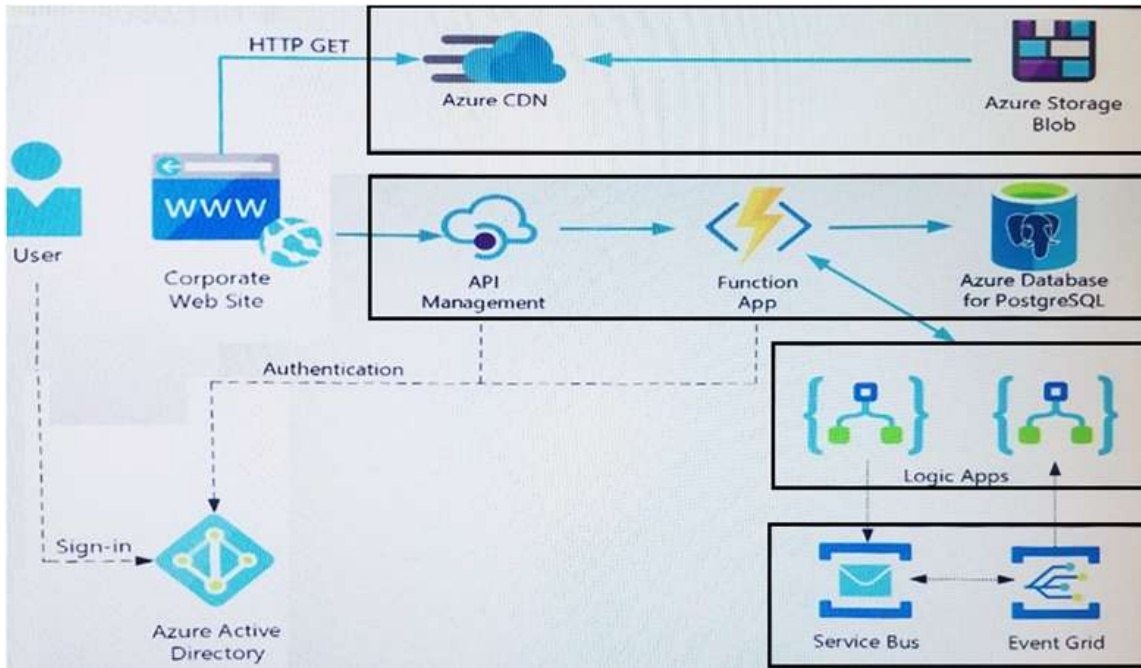
The company has a public website located at <http://www.cpandl.com/>. The site is a single-page web application that runs in Azure App Service on Linux. The website uses files stored in Azure Storage and cached in Azure Content Delivery Network (CDN) to serve static content.

API Management and Azure Function App functions are used to process and store data in Azure Database for PostgreSQL. API Management is used to broker communications to the Azure Function app functions for Logic app integration. Logic apps are used to orchestrate the data processing while Service Bus and Event Grid handle messaging and events.

The solution uses Application Insights, Azure Monitor, and Azure Key Vault.

Architecture diagram

The company has several applications and services that support their business. The company plans to implement serverless computing where possible. The overall architecture is shown below.



User authentication

The following steps detail the user authentication process:

7. The user selects **Sign in** in the website.
8. The browser redirects the user to the Azure Active Directory (Azure AD) sign in page.
9. The user signs in.
10. Azure AD redirects the user's session back to the web application. The URL includes an access token.
11. The web application calls an API and includes the access token in the authentication header. The application ID is sent as the audience ('aud') claim in the access token.
12. The back-end API validates the access token.

Requirements

Corporate website

- Communications and content must be secured by using SSL.
- Communications must use HTTPS.
- Data must be replicated to a secondary region and three availability zones.
- Data storage costs must be minimized.

Azure Database for PostgreSQL

The database connection string is stored in Azure Key Vault with the following attributes:

- Azure Key Vault name: cpandlkeyvault
- Secret name: PostgreSQLConn
- Id: 80df3e46ffcd4f1cb187f79905e9a1e8

The connection information is updated frequently. The application must always use the latest information to connect to the database.

Azure Service Bus and Azure Event Grid

- Azure Event Grid must use Azure Service Bus for queue-based load leveling.
- Events in Azure Event Grid must be routed directly to Service Bus queues for use in buffering.
- Events from Azure Service Bus and other Azure services must continue to be routed to Azure Event Grid for processing.

Security

- All SSL certificates and credentials must be stored in Azure Key Vault.
- File access must restrict access by IP, protocol, and Azure AD rights.
- All user accounts and processes must receive only those privileges which are essential to perform their intended function.

Compliance

Auditing of the file updates and transfers must be enabled to comply with General Data Protection Regulation (GDPR). The file updates must be read-only, stored in the order in which they occurred, include only create, update, delete, and copy operations, and be retained for compliance reasons.

Issues

Corporate website

While testing the site, the following error message displays:

CryptographicException: The system cannot find the file specified.

Function app

You perform local testing for the RequestUserApproval function. The following error message displays:

'Timeout value of 00:10:00 exceeded by function: RequestUserApproval'

The same error message displays when you test the function in an Azure development environment when you run the following Kusto query:

```
FunctionAppLogs  
| where FunctionName == "RequestUserApproval"
```

Logic app

You test the Logic app in a development environment. The following error message displays:

'400 Bad Request'

Troubleshooting of the error shows an HttpTrigger action to call the RequestUserApproval function.

Code

Corporate website

Security.cs:

```
SC01 public class Security  
SC02 {  
SC03 var bytes = System.IO.File.ReadAllBytes("~/var/ssl/private");  
SC04 var cert = new System.Security.Cryptography.X509Certificate2(bytes);  
SC05 var certName = cert.FriendlyName;  
SC06 }
```

Function app

RequestUserApproval.cs:

```
RA01 public static class RequestUserApproval  
RA02 {  
RA03 [FunctionName("RequestUserApproval")]  
RA04 public static async Task<ActionResult> Run(  
RA05 [HttpTrigger(AuthorizationLevel.Function, "get", "post", Route = null)] HttpRequest req,  
RA06 ILogger log)  
RA07 {  
RA08 log.LogInformation("RequestUserApproval function processed a request.");  
RA09 ...  
RA10 return ProcessRequest(req)  
RA11 ? (ActionResult)new OkObjectResult($"User approval processed")  
RA12 : new BadRequestObjectResult("Failed to process user approval");  
RA13 }  
RA14 private static bool ProcessRequest(HttpRequest req)  
RA15 {  
RA16 ...  
RA17 }
```

You need to authenticate the user to the corporate website as indicated by the architectural diagram.

Which two values should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. ID token signature
- B. ID token claims
- C. HTTP response code
- D. Azure AD endpoint URI
- E. Azure AD tenant ID

Answer: AD

Explanation:

A: Claims in access tokens

JWTs (JSON Web Tokens) are split into three pieces:

[AZ-204 Exam Dumps](#) [AZ-204 Exam Questions](#) [AZ-204 PDF Dumps](#) [AZ-204 VCE Dumps](#)

<https://www.braindump2go.com/az-204.html>

Header - Provides information about how to validate the token including information about the type of token and how it was signed.

Payload - Contains all of the important data about the user or app that is attempting to call your service.

Signature - Is the raw material used to validate the token.

E: Your client can get an access token from either the v1.0 endpoint or the v2.0 endpoint using a variety of protocols.

Scenario: User authentication (see step 5 below)

The following steps detail the user authentication process:

1. The user selects Sign in in the website.
2. The browser redirects the user to the Azure Active Directory (Azure AD) sign in page.
3. The user signs in.
4. Azure AD redirects the user's session back to the web application. The URL includes an access token.
5. The web application calls an API and includes the access token in the authentication header. The application ID is sent as the audience ('aud') claim in the access token.
6. The back-end API validates the access token.

Reference:

<https://docs.microsoft.com/en-us/azure/api-management/api-management-access-restriction-policies>

QUESTION 69

Case Study 3 - City Power & Light

Background

City Power & Light company provides electrical infrastructure monitoring solutions for homes and businesses. The company is migrating solutions to Azure.

Current environment

Architecture overview

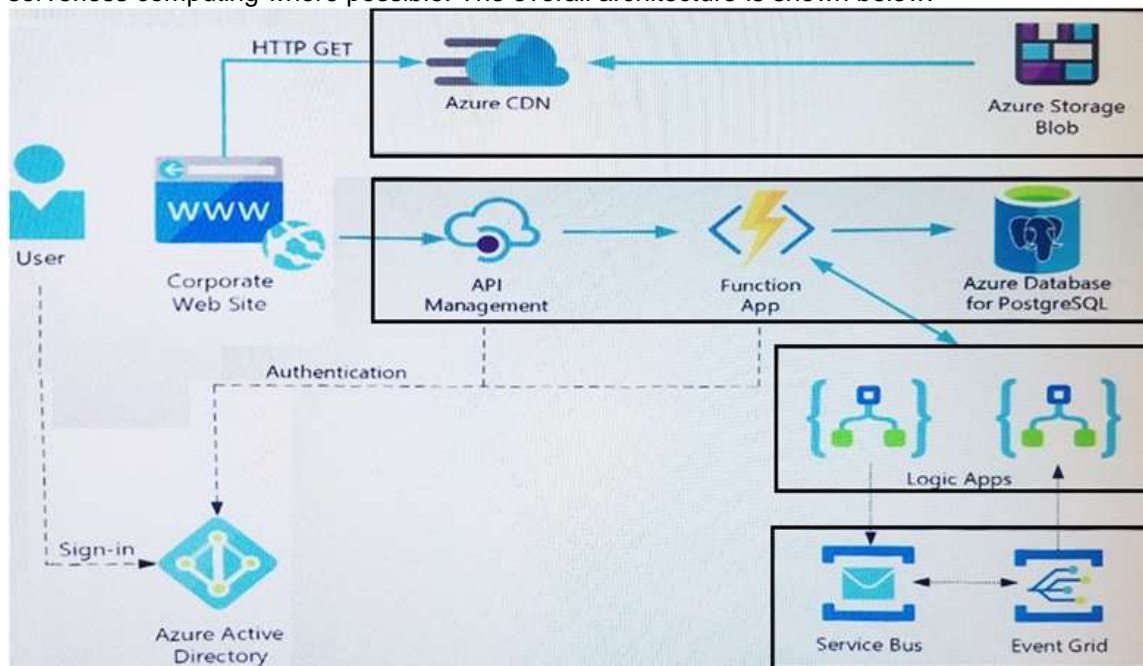
The company has a public website located at <http://www.cpandl.com/>. The site is a single-page web application that runs in Azure App Service on Linux. The website uses files stored in Azure Storage and cached in Azure Content Delivery Network (CDN) to serve static content.

API Management and Azure Function App functions are used to process and store data in Azure Database for PostgreSQL. API Management is used to broker communications to the Azure Function app functions for Logic app integration. Logic apps are used to orchestrate the data processing while Service Bus and Event Grid handle messaging and events.

The solution uses Application Insights, Azure Monitor, and Azure Key Vault.

Architecture diagram

The company has several applications and services that support their business. The company plans to implement serverless computing where possible. The overall architecture is shown below.



User authentication

The following steps detail the user authentication process:

[AZ-204 Exam Dumps](#) [AZ-204 Exam Questions](#) [AZ-204 PDF Dumps](#) [AZ-204 VCE Dumps](#)

<https://www.braindump2go.com/az-204.html>

13. The user selects **Sign in** in the website.
14. The browser redirects the user to the Azure Active Directory (Azure AD) sign in page.
15. The user signs in.
16. Azure AD redirects the user's session back to the web application. The URL includes an access token.
17. The web application calls an API and includes the access token in the authentication header. The application ID is sent as the audience ('aud') claim in the access token.
18. The back-end API validates the access token.

Requirements**Corporate website**

- Communications and content must be secured by using SSL.
- Communications must use HTTPS.
- Data must be replicated to a secondary region and three availability zones.
- Data storage costs must be minimized.

Azure Database for PostgreSQL

The database connection string is stored in Azure Key Vault with the following attributes:

- Azure Key Vault name: cpandkeyvault
- Secret name: PostgreSQLConn
- Id: 80df3e46ffcd4f1cb187f79905e9a1e8

The connection information is updated frequently. The application must always use the latest information to connect to the database.

Azure Service Bus and Azure Event Grid

- Azure Event Grid must use Azure Service Bus for queue-based load leveling.
- Events in Azure Event Grid must be routed directly to Service Bus queues for use in buffering.
- Events from Azure Service Bus and other Azure services must continue to be routed to Azure Event Grid for processing.

Security

- All SSL certificates and credentials must be stored in Azure Key Vault.
- File access must restrict access by IP, protocol, and Azure AD rights.
- All user accounts and processes must receive only those privileges which are essential to perform their intended function.

Compliance

Auditing of the file updates and transfers must be enabled to comply with General Data Protection Regulation (GDPR). The file updates must be read-only, stored in the order in which they occurred, include only create, update, delete, and copy operations, and be retained for compliance reasons.

Issues**Corporate website**

While testing the site, the following error message displays:

CryptographicException: The system cannot find the file specified.

Function app

You perform local testing for the RequestUserApproval function. The following error message displays:

'Timeout value of 00:10:00 exceeded by function: RequestUserApproval'

The same error message displays when you test the function in an Azure development environment when you run the following Kusto query:

```
FunctionAppLogs  
| where FunctionName == "RequestUserApproval"
```

Logic app

You test the Logic app in a development environment. The following error message displays:

'400 Bad Request'

Troubleshooting of the error shows an HttpTrigger action to call the RequestUserApproval function.

Code**Corporate website**

Security.cs:

```
SC01 public class Security
SC02 {
SC03     var bytes = System.IO.File.ReadAllBytes("~/var/ssl/private");
SC04     var cert = new System.Security.Cryptography.X509Certificate2(bytes);
SC05     var certName = cert.FriendlyName;
SC06 }
```

Function app

RequestUserApproval.cs:

```
RA01 public static class RequestUserApproval
RA02 {
RA03     [FunctionName("RequestUserApproval")]
RA04     public static async Task<IActionResult> Run(
RA05     [HttpTrigger(AuthorizationLevel.Function, "get", "post", Route = null)] HttpRequest req,
RA06     ILogger log)
RA07     {
RA08         log.LogInformation("RequestUserApproval function processed a request.");
RA09         return ProcessRequest(req);
RA10     }
RA11     ? (ActionResult)new OkObjectResult($"User approval processed")
RA12     : new BadRequestObjectResult("Failed to process user approval");
RA13 }
RA14 private static bool ProcessRequest(HttpRequest req)
RA15 {
RA16     ...
RA17 }
```

You need to investigate the Azure Function app error message in the development environment. What should you do?

- A. Connect Live Metrics Stream from Application Insights to the Azure Function app and filter the metrics.
- B. Create a new Azure Log Analytics workspace and instrument the Azure Function app with Application Insights.
- C. Update the Azure Function app with extension methods from Microsoft.Extensions.Logging to log events by using the log instance.
- D. Add a new diagnostic setting to the Azure Function app to send logs to Log Analytics.

Answer: A**Explanation:**

Azure Functions offers built-in integration with Azure Application Insights to monitor functions.

The following areas of Application Insights can be helpful when evaluating the behavior, performance, and errors in your functions:

Live Metrics: View metrics data as it's created in near real-time.

Failures

Performance

Metrics

Reference:

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-monitoring>

QUESTION 70**Case Study 3 - City Power & Light****Background**

City Power & Light company provides electrical infrastructure monitoring solutions for homes and businesses. The company is migrating solutions to Azure.

Current environment**Architecture overview**

The company has a public website located at <http://www.cpandl.com/>. The site is a single-page web application that runs in Azure App Service on Linux. The website uses files stored in Azure Storage and cached in Azure Content Delivery Network (CDN) to serve static content.

API Management and Azure Function App functions are used to process and store data in Azure Database for PostgreSQL. API Management is used to broker communications to the Azure Function app functions for Logic app

[AZ-204 Exam Dumps](#) [AZ-204 Exam Questions](#) [AZ-204 PDF Dumps](#) [AZ-204 VCE Dumps](#)

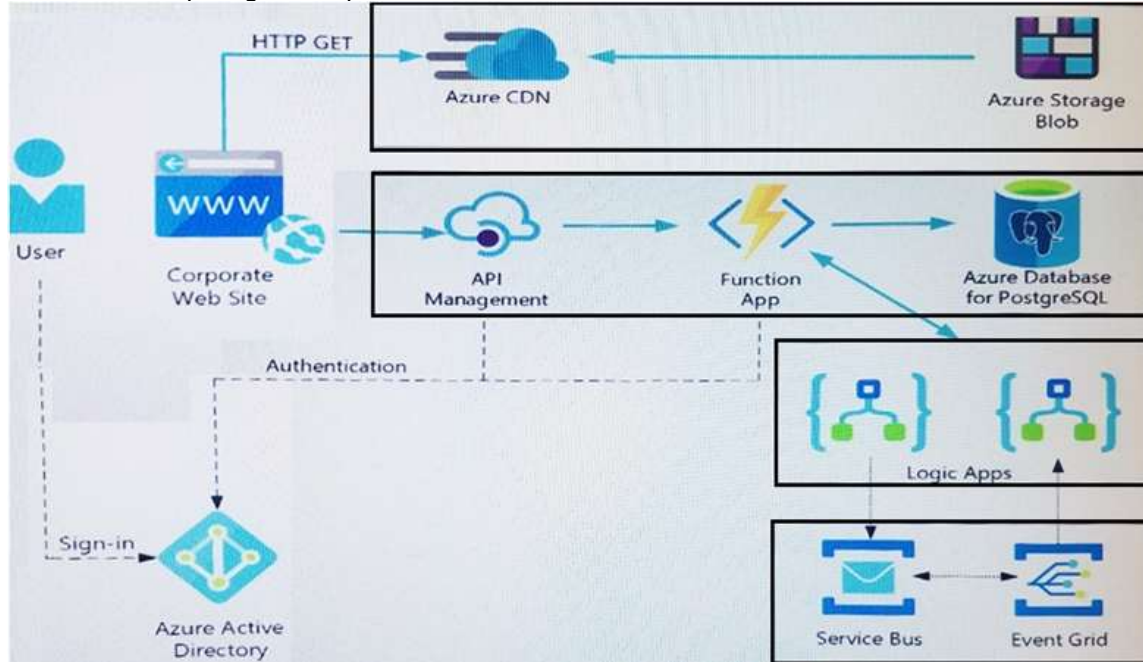
<https://www.braindump2go.com/az-204.html>

integration. Logic apps are used to orchestrate the data processing while Service Bus and Event Grid handle messaging and events.

The solution uses Application Insights, Azure Monitor, and Azure Key Vault.

Architecture diagram

The company has several applications and services that support their business. The company plans to implement serverless computing where possible. The overall architecture is shown below.



User authentication

The following steps detail the user authentication process:

19. The user selects **Sign in** in the website.
20. The browser redirects the user to the Azure Active Directory (Azure AD) sign in page.
21. The user signs in.
22. Azure AD redirects the user's session back to the web application. The URL includes an access token.
23. The web application calls an API and includes the access token in the authentication header. The application ID is sent as the audience ('aud') claim in the access token.
24. The back-end API validates the access token.

Requirements

Corporate website

- Communications and content must be secured by using SSL.
- Communications must use HTTPS.
- Data must be replicated to a secondary region and three availability zones.
- Data storage costs must be minimized.

Azure Database for PostgreSQL

The database connection string is stored in Azure Key Vault with the following attributes:

- Azure Key Vault name: cpandkeyvault
- Secret name: PostgreSQLConn
- Id: 80df3e46ffcd4f1cb187f79905e9a1e8

The connection information is updated frequently. The application must always use the latest information to connect to the database.

Azure Service Bus and Azure Event Grid

- Azure Event Grid must use Azure Service Bus for queue-based load leveling.
- Events in Azure Event Grid must be routed directly to Service Bus queues for use in buffering.
- Events from Azure Service Bus and other Azure services must continue to be routed to Azure Event Grid for processing.

Security

- All SSL certificates and credentials must be stored in Azure Key Vault.
- File access must restrict access by IP, protocol, and Azure AD rights.

[AZ-204 Exam Dumps](#) [AZ-204 Exam Questions](#) [AZ-204 PDF Dumps](#) [AZ-204 VCE Dumps](#)

- All user accounts and processes must receive only those privileges which are essential to perform their intended function.

Compliance

Auditing of the file updates and transfers must be enabled to comply with General Data Protection Regulation (GDPR). The file updates must be read-only, stored in the order in which they occurred, include only create, update, delete, and copy operations, and be retained for compliance reasons.

Issues**Corporate website**

While testing the site, the following error message displays:

CryptographicException: The system cannot find the file specified.

Function app

You perform local testing for the RequestUserApproval function. The following error message displays:

'Timeout value of 00:10:00 exceeded by function: RequestUserApproval'

The same error message displays when you test the function in an Azure development environment when you run the following Kusto query:

```
FunctionAppLogs  
| where FunctionName == "RequestUserApproval"
```

Logic app

You test the Logic app in a development environment. The following error message displays:

'400 Bad Request'

Troubleshooting of the error shows an HttpTrigger action to call the RequestUserApproval function.

Code**Corporate website**

Security.cs:

```
SC01 public class Security  
SC02 {  
SC03     var bytes = System.IO.File.ReadAllBytes("~/var/ssl/private");  
SC04     var cert = new System.Security.Cryptography.X509Certificate2(bytes);  
SC05     var certName = cert.FriendlyName;  
SC06 }
```

Function app

RequestUserApproval.cs:

```
RA01 public static class RequestUserApproval  
RA02 {  
RA03     [FunctionName("RequestUserApproval")]  
RA04     public static async Task<ActionResult> Run(  
RA05         [HttpTrigger(AuthorizationLevel.Function, "get", "post", Route = null)] HttpRequest req,  
RA06         ILogger log)  
RA07     {  
RA08         log.LogInformation("RequestUserApproval function processed a request.");  
RA09         return ProcessRequest(req)  
RA10             ? (ActionResult)new OkObjectResult($"User approval processed")  
RA11             : new BadRequestObjectResult("Failed to process user approval");  
RA12     }  
RA13     private static bool ProcessRequest(HttpRequest req)  
RA14     {  
RA15         ...  
RA16     }  
RA17 }
```

Hotspot Question

You need to configure the Account Kind, Replication, and Storage tier options for the corporate website's Azure Storage account.

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

NOTE: Each correct selection is worth one point.

Create storage account



Basics Advanced Tags Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more](#)

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription

* Resource group

[Create new](#)

INSTANCE DETAILS

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

* Storage account name

* Location

Performance ☒ Standard ☐ Premium

Account kind

Replication

Access tier (default) ☐ Cool ☐ Hot

Answer:

Create storage account



[Basics](#) [Advanced](#) [Tags](#) [Review + create](#)

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more](#)

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription

* Resource group

[Create new](#)

INSTANCE DETAILS

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

* Storage account name

* Location

Performance ☒ Standard ☐ Premium

Account kind

Replication

Access tier (default) ☐ Cool ☐ Hot

Explanation:

Account Kind: StorageV2 (general-purpose v2)

Scenario: Azure Storage blob will be used (refer to the exhibit). Data storage costs must be minimized.

General-purpose v2 accounts: Basic storage account type for blobs, files, queues, and tables.

Recommended for most scenarios using Azure Storage.

Incorrect Answers:

BlockBlobStorage accounts: Storage accounts with premium performance characteristics for block blobs and append blobs. Recommended for scenarios with high transactions rates, or scenarios that use smaller objects or require consistently low storage latency.

General-purpose v1 accounts: Legacy account type for blobs, files, queues, and tables. Use general-purpose v2 accounts instead when possible.

Replication: Geo-redundant Storage

Scenario: Data must be replicated to a secondary region and three availability zones.

Geo-redundant storage (GRS) copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in the secondary region.

[AZ-204 Exam Dumps](#) [AZ-204 Exam Questions](#) [AZ-204 PDF Dumps](#) [AZ-204 VCE Dumps](#)

<https://www.braindump2go.com/az-204.html>

Incorrect Answers:

Geo-zone-redundant storage (GZRS), but it would be more costly.

Storage tier: Cool

Data storage costs must be minimized.

Note: Azure storage offers different access tiers, which allow you to store blob object data in the most cost-effective manner. The available access tiers include:

Hot - Optimized for storing data that is accessed frequently. Cool - Optimized for storing data that is infrequently accessed and stored for at least 30 days.

Reference:

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

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

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers?tabs=azure-portal>

QUESTION 71

Case Study 3 - City Power & Light

Background

City Power & Light company provides electrical infrastructure monitoring solutions for homes and businesses. The company is migrating solutions to Azure.

Current environment

Architecture overview

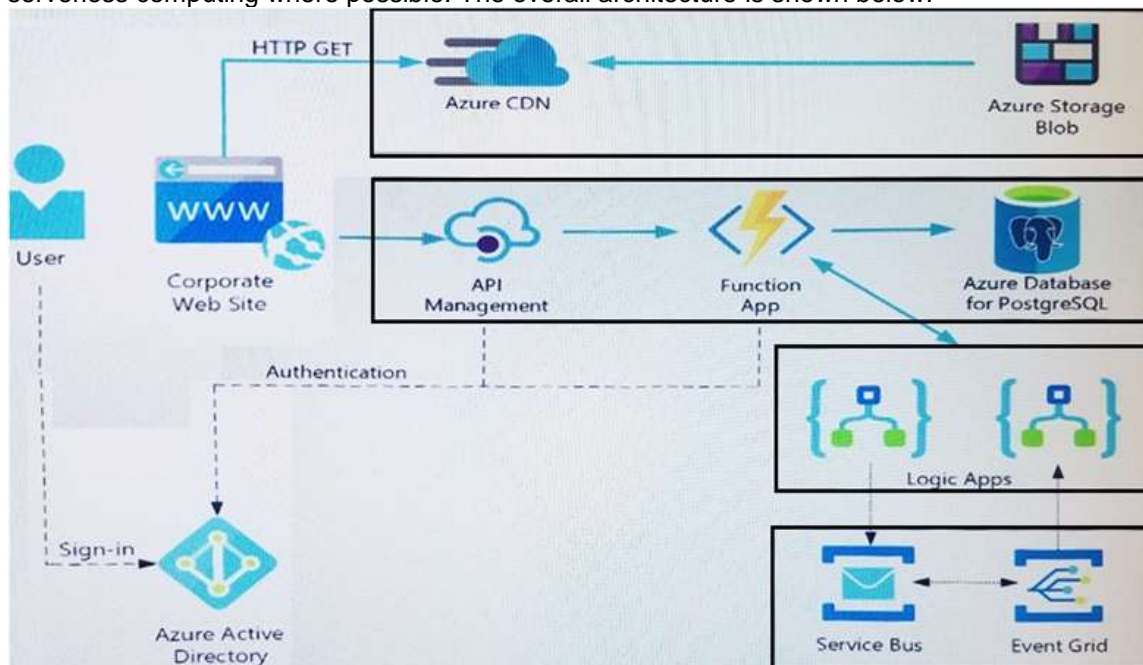
The company has a public website located at <http://www.cpanel.com/>. The site is a single-page web application that runs in Azure App Service on Linux. The website uses files stored in Azure Storage and cached in Azure Content Delivery Network (CDN) to serve static content.

API Management and Azure Function App functions are used to process and store data in Azure Database for PostgreSQL. API Management is used to broker communications to the Azure Function app functions for Logic app integration. Logic apps are used to orchestrate the data processing while Service Bus and Event Grid handle messaging and events.

The solution uses Application Insights, Azure Monitor, and Azure Key Vault.

Architecture diagram

The company has several applications and services that support their business. The company plans to implement serverless computing where possible. The overall architecture is shown below.



User authentication

The following steps detail the user authentication process:

25. The user selects **Sign in** in the website.

26. The browser redirects the user to the Azure Active Directory (Azure AD) sign in page.

27. The user signs in.

28. Azure AD redirects the user's session back to the web application. The URL includes an access token.

29. The web application calls an API and includes the access token in the authentication header. The application ID is sent as the audience ('aud') claim in the access token.

30. The back-end API validates the access token.

Requirements**Corporate website**

- Communications and content must be secured by using SSL.
- Communications must use HTTPS.
- Data must be replicated to a secondary region and three availability zones.
- Data storage costs must be minimized.

Azure Database for PostgreSQL

The database connection string is stored in Azure Key Vault with the following attributes:

- Azure Key Vault name: cpandlkeyvault
- Secret name: PostgreSQLConn
- Id: 80df3e46ffcd4f1cb187f79905e9a1e8

The connection information is updated frequently. The application must always use the latest information to connect to the database.

Azure Service Bus and Azure Event Grid

- Azure Event Grid must use Azure Service Bus for queue-based load leveling.
- Events in Azure Event Grid must be routed directly to Service Bus queues for use in buffering.
- Events from Azure Service Bus and other Azure services must continue to be routed to Azure Event Grid for processing.

Security

- All SSL certificates and credentials must be stored in Azure Key Vault.
- File access must restrict access by IP, protocol, and Azure AD rights.
- All user accounts and processes must receive only those privileges which are essential to perform their intended function.

Compliance

Auditing of the file updates and transfers must be enabled to comply with General Data Protection Regulation (GDPR). The file updates must be read-only, stored in the order in which they occurred, include only create, update, delete, and copy operations, and be retained for compliance reasons.

Issues**Corporate website**

While testing the site, the following error message displays:

CryptographicException: The system cannot find the file specified.

Function app

You perform local testing for the RequestUserApproval function. The following error message displays:

'Timeout value of 00:10:00 exceeded by function: RequestUserApproval'

The same error message displays when you test the function in an Azure development environment when you run the following Kusto query:

```
FunctionAppLogs  
| where FunctionName == "RequestUserApproval"
```

Logic app

You test the Logic app in a development environment. The following error message displays:

'400 Bad Request'

Troubleshooting of the error shows an HttpTrigger action to call the RequestUserApproval function.

Code**Corporate website**

Security.cs:

```
SC01 public class Security  
SC02 {  
SC03 var bytes = System.IO.File.ReadAllBytes("~/var/ssl/private");  
SC04 var cert = new System.Security.Cryptography.X509Certificate2(bytes);  
SC05 var certName = cert.FriendlyName;  
SC06 }
```

Function app

RequestUserApproval.cs:

```

RA01 public static class RequestUserApproval
RA02 {
RA03 [FunctionName("RequestUserApproval")]
RA04 public static async Task<IActionResult> Run(
RA05 [HttpTrigger(AuthorizationLevel.Function, "get", "post", Route = null)] HttpRequest req,
RA06 ILogger log)
RA07 {
RA08     log.LogInformation("RequestUserApproval function processed a request.");
RA09     ...
RA10     return ProcessRequest(req)
RA11     ? (ActionResult)new OkObjectResult($"User approval processed")
RA12     : new BadRequestObjectResult("Failed to process user approval");
RA13 }
RA14 private static bool ProcessRequest(HttpRequest req)
RA15 {
RA16     ...
RA17 }

```

Hotspot Question

You need to retrieve the database connection string.

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

NOTE: Each correct selection is worth one point.

Answer Area

REST API Endpoint:

https:// /

Variable type to access Azure Key Vault secret values:

Answer:

Answer Area

REST API Endpoint:

https:// /

Variable type to access Azure Key Vault secret values:

Explanation:

Azure database connection string retrieve REST API vault.azure.net/secrets/

Box 1: cpandlkeyvault

We specify the key vault, cpandlkeyvault.

Scenario: The database connection string is stored in Azure Key Vault with the following attributes:

Azure Key Vault name: cpandlkeyvault

Secret name: PostgreSQLConn

Id: 80df3e46ffcd4f1cb187f79905e9a1e8

Box 2: PostgreSQLConn

We specify the secret, PostgreSQLConn

Example, sample request:

https://myvault.vault.azure.net/secrets/mysecretname/4387e9f3d6e14c459867679a90fd0f79?api-version=7.1

Box 3: Querystring

Reference:

<https://docs.microsoft.com/en-us/rest/api/keyvault/getsecret/getsecret>

QUESTION 72

Case Study 3 - City Power & Light

Background

City Power & Light company provides electrical infrastructure monitoring solutions for homes and businesses. The company is migrating solutions to Azure.

Current environment

Architecture overview

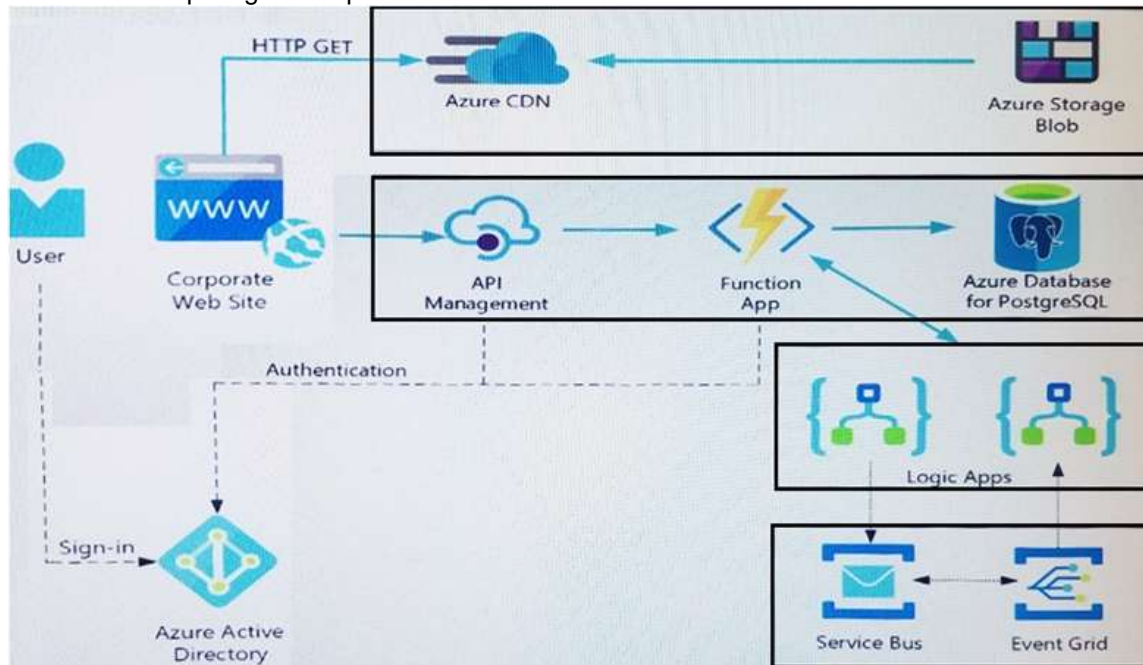
The company has a public website located at <http://www.cpandl.com/>. The site is a single-page web application that runs in Azure App Service on Linux. The website uses files stored in Azure Storage and cached in Azure Content Delivery Network (CDN) to serve static content.

API Management and Azure Function App functions are used to process and store data in Azure Database for PostgreSQL. API Management is used to broker communications to the Azure Function app functions for Logic app integration. Logic apps are used to orchestrate the data processing while Service Bus and Event Grid handle messaging and events.

The solution uses Application Insights, Azure Monitor, and Azure Key Vault.

Architecture diagram

The company has several applications and services that support their business. The company plans to implement serverless computing where possible. The overall architecture is shown below.



User authentication

The following steps detail the user authentication process:

31. The user selects **Sign in** in the website.
32. The browser redirects the user to the Azure Active Directory (Azure AD) sign in page.
33. The user signs in.
34. Azure AD redirects the user's session back to the web application. The URL includes an access token.
35. The web application calls an API and includes the access token in the authentication header. The application ID is sent as the audience ('aud') claim in the access token.
36. The back-end API validates the access token.

Requirements

Corporate website

- Communications and content must be secured by using SSL.
- Communications must use HTTPS.
- Data must be replicated to a secondary region and three availability zones.
- Data storage costs must be minimized.

Azure Database for PostgreSQL

The database connection string is stored in Azure Key Vault with the following attributes:

[AZ-204 Exam Dumps](#) [AZ-204 Exam Questions](#) [AZ-204 PDF Dumps](#) [AZ-204 VCE Dumps](#)

- Azure Key Vault name: cpandlkeyvault
- Secret name: PostgreSQLConn
- Id: 80df3e46ffcd4f1cb187f79905e9a1e8

The connection information is updated frequently. The application must always use the latest information to connect to the database.

Azure Service Bus and Azure Event Grid

- Azure Event Grid must use Azure Service Bus for queue-based load leveling.
- Events in Azure Event Grid must be routed directly to Service Bus queues for use in buffering.
- Events from Azure Service Bus and other Azure services must continue to be routed to Azure Event Grid for processing.

Security

- All SSL certificates and credentials must be stored in Azure Key Vault.
- File access must restrict access by IP, protocol, and Azure AD rights.
- All user accounts and processes must receive only those privileges which are essential to perform their intended function.

Compliance

Auditing of the file updates and transfers must be enabled to comply with General Data Protection Regulation (GDPR). The file updates must be read-only, stored in the order in which they occurred, include only create, update, delete, and copy operations, and be retained for compliance reasons.

Issues**Corporate website**

While testing the site, the following error message displays:

CryptographicException: The system cannot find the file specified.

Function app

You perform local testing for the RequestUserApproval function. The following error message displays:

'Timeout value of 00:10:00 exceeded by function: RequestUserApproval'

The same error message displays when you test the function in an Azure development environment when you run the following Kusto query:

```
FunctionAppLogs  
| where FunctionName == "RequestUserApproval"
```

Logic app

You test the Logic app in a development environment. The following error message displays:

'400 Bad Request'

Troubleshooting of the error shows an HttpTrigger action to call the RequestUserApproval function.

Code**Corporate website**

Security.cs:

```
SC01 public class Security  
SC02 {  
SC03 var bytes = System.IO.File.ReadAllBytes("~/var/ssl/private");  
SC04 var cert = new System.Security.Cryptography.X509Certificate2(bytes);  
SC05 var certName = cert.FriendlyName;  
SC06 }
```

Function app

RequestUserApproval.cs:

```

RA01 public static class RequestUserApproval
RA02 {
RA03     [FunctionName("RequestUserApproval")]
RA04     public static async Task<IActionResult> Run(
RA05     [HttpTrigger(AuthorizationLevel.Function, "get", "post", Route = null)] HttpRequest req,
RA06     ILogger log)
RA07     {
RA08         log.LogInformation("RequestUserApproval function processed a request.");
RA09         ...
RA10         return ProcessRequest(req)
RA11         ? (ActionResult)new OkObjectResult($"User approval processed")
RA12         : new BadRequestObjectResult("Failed to process user approval");
RA13     }
RA14     private static bool ProcessRequest(HttpRequest req)
RA15     {
RA16         ...
RA17     }

```

Drag and Drop Question

You need to correct the corporate website error.

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

Actions

Answer Area

Upload the certificate to Azure Key Vault.

Update line SC05 of Security.cs to include error handling and then redeploy the code.

Update line SC03 of Security.cs to include a using statement and then re-deploy the code.

Add the certificate thumbprint to the WEBSITE_LOAD_CERTIFICATES app setting.

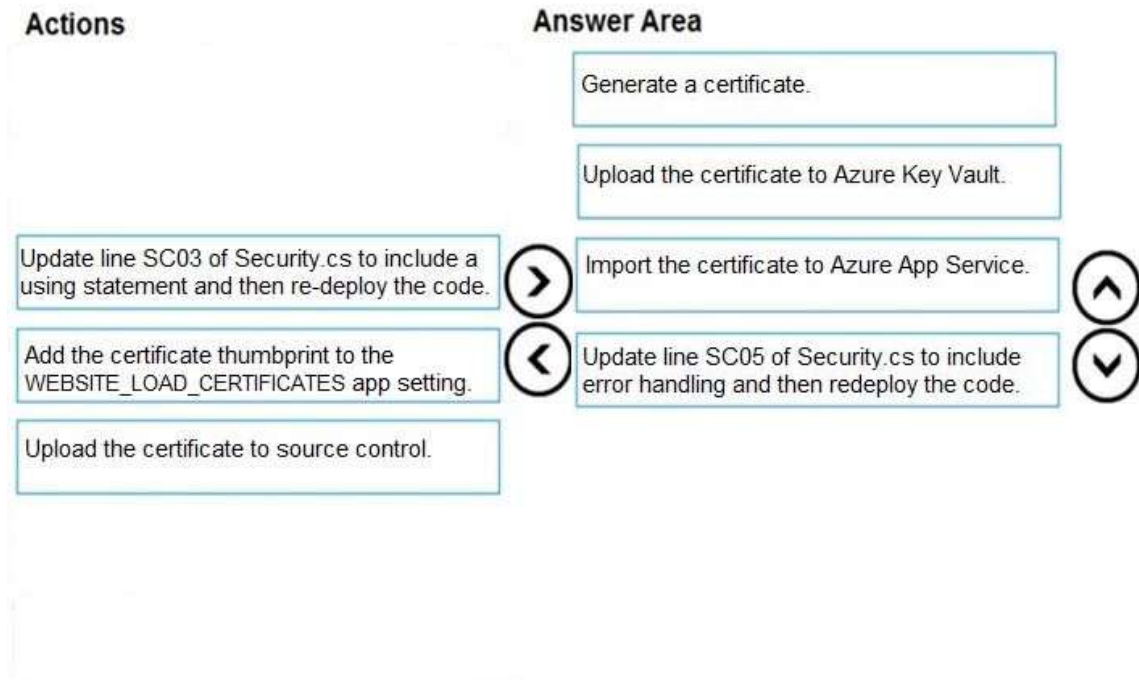
Upload the certificate to source control.

Import the certificate to Azure App Service.

Generate a certificate.



Answer:

**Explanation:**

Scenario: Corporate website

While testing the site, the following error message displays:

CryptographicException: The system cannot find the file specified.

Step 1: Generate a certificate

Step 2: Upload the certificate to Azure Key Vault

Scenario: All SSL certificates and credentials must be stored in Azure Key Vault.

Step 3: Import the certificate to Azure App Service

Step 4: Update line SC05 of Security.cs to include error handling and then redeploy the code

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate>