|  |  |
| --- | --- |
| **Case** | **1 : mijnaz204@outlook.com** |
| Description | Current environment - Windows Server 2016 virtual machine This virtual machine (VM) runs BizTalk Server 2016. The VM runs the following workflows: Ocean Transport "" This workflow gathers and validates container information including container contents and arrival notices at various shipping ports. Inland Transport "" This workflow gathers and validates trucking information including fuel usage, number of stops, and routes. The VM supports the following REST API calls: Container API "" This API provides container information including weight, contents, and other attributes. Location API "" This API provides location information regarding shipping ports of call and trucking stops. Shipping REST API "" This API provides shipping information for use and display on the shipping website.  Shipping Data - The application uses MongoDB JSON document storage database for all container and transport information.  Shipping Web Site - The site displays shipping container tracking information and container contents. The site is located at http://shipping.wideworldimporters.com/  Proposed solution - The on-premises shipping application must be moved to Azure. The VM has been migrated to a new Standard\_D16s\_v3 Azure VM by using Azure Site Recovery and must remain running in Azure to complete the BizTalk component migrations. You create a Standard\_D16s\_v3 Azure VM to host BizTalk Server. The Azure architecture diagram for the proposed solution is shown below:    Requirements -  Shipping Logic app - The Shipping Logic app must meet the following requirements: Support the ocean transport and inland transport workflows by using a Logic App. Support industry-standard protocol X12 message format for various messages including vessel content details and arrival notices. Secure resources to the corporate VNet and use dedicated storage resources with a fixed costing model. Maintain on-premises connectivity to support legacy applications and final BizTalk migrations.  Shipping Function app - Implement secure function endpoints by using app-level security and include Azure Active Directory (Azure AD).  REST APIs - The REST API"™s that support the solution must meet the following requirements: Secure resources to the corporate VNet. Allow deployment to a testing location within Azure while not incurring additional costs. Automatically scale to double capacity during peak shipping times while not causing application downtime. Minimize costs when selecting an Azure payment model.  Shipping data - Data migration from on-premises to Azure must minimize costs and downtime.  Shipping website - Use Azure Content Delivery Network (CDN) and ensure maximum performance for dynamic content while minimizing latency and costs.  Issues -  Windows Server 2016 VM - The VM shows high network latency, jitter, and high CPU utilization. The VM is critical and has not been backed up in the past. The VM must enable a quick restore from a 7-day snapshot to include in-place restore of disks in case of failure.  Shipping website and REST APIs - The following error message displays while you are testing the website: Failed to load http://test-shippingapi.wideworldimporters.com/: No 'Access-Control-Allow-Origin' header is present on the requested resource. Origin 'http://test.wideworldimporters.com/' is therefore not allowed access. |
| Question 1 | You need to configure Azure CDN for the Shipping web site. Which configuration options should you use? |
| Answer |  |
| Explanation | Scenario: Shipping website - Use Azure Content Delivery Network (CDN) and ensure maximum performance for dynamic content while minimizing latency and costs.  Tier: Standard -  Profile: Akamai - Optimization: Dynamic site acceleration Dynamic site acceleration (DSA) is available for Azure CDN Standard from Akamai, Azure CDN Standard from Verizon, and Azure CDN Premium from Verizon profiles. DSA includes various techniques that benefit the latency and performance of dynamic content. Techniques include route and network optimization, TCP optimization, and more. You can use this optimization to accelerate a web app that includes numerous responses that aren't cacheable. Examples are search results, checkout transactions, or real-time data. You can continue to use core Azure CDN caching capabilities for static data. Reference: <https://docs.microsoft.com/en-us/azure/cdn/cdn-optimization-overview> |
| Question 2 | You need to correct the VM issues. Which tools should you use? |
| Answer |  |
| Explanation | Box 1: Azure Backup - The VM is critical and has not been backed up in the past. The VM must enable a quick restore from a 7-day snapshot to include in-place restore of disks in case of failure. In-Place restore of disks in IaaS VMs is a feature of Azure Backup. Performance: Accelerated Networking Scenario: The VM shows high network latency, jitter, and high CPU utilization.  Box 2: Accelerated networking - The VM shows high network latency, jitter, and high CPU utilization. Accelerated networking enables single root I/O virtualization (SR-IOV) to a VM, greatly improving its networking performance. This high-performance path bypasses the host from the datapath, reducing latency, jitter, and CPU utilization, for use with the most demanding network workloads on supported VM types. Reference: <https://azure.microsoft.com/en-us/blog/an-easy-way-to-bring-back-your-azure-vm-with-in-place-restore/> |
| Question 3 | You need to support the requirements for the Shipping Logic App. What should you use? |
| Answer | * A. Azure Active Directory Application Proxy * B. Site-to-Site (S2S) VPN connection * C. On-premises Data Gateway * D. Point-to-Site (P2S) VPN connection |
| Explanation | Before you can connect to on-premises data sources from Azure Logic Apps, download and install the on-premises data gateway on a local computer. The gateway works as a bridge that provides quick data transfer and encryption between data sources on premises (not in the cloud) and your logic apps. The gateway supports BizTalk Server 2016. Note: Microsoft have now fully incorporated the Azure BizTalk Services capabilities into Logic Apps and Azure App Service Hybrid Connections. Logic Apps Enterprise Integration pack bring some of the enterprise B2B capabilities like AS2 and X12, EDI standards support Scenario: The Shipping Logic app must meet the following requirements: ✑ Support the ocean transport and inland transport workflows by using a Logic App. ✑ Support industry-standard protocol X12 message format for various messages including vessel content details and arrival notices. ✑ Secure resources to the corporate VNet and use dedicated storage resources with a fixed costing model. ✑ Maintain on-premises connectivity to support legacy applications and final BizTalk migrations. Reference: <https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-gateway-install>  Connect to and consume Azure services and third-party services |
| Question 4 | You need to secure the Shipping Function app.  How should you configure the app? To answer, select the appropriate options in the answer area |
| Answer |  |
| Explanation | Scenario: Shipping Function app: Implement secure function endpoints by using app-level security and include Azure Active Directory (Azure AD).  Box 1: Function - Box 2: JSON based Token (JWT) Azure AD uses JSON based tokens (JWTs) that contain claims  Box 3: HTTP - How a web app delegates sign-in to Azure AD and obtains a token User authentication happens via the browser. The OpenID protocol uses standard HTTP protocol messages. Reference: <https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-scenarios> |
| Question 5 | You need to secure the Shipping Logic App. What should you use? |
| Answer | * A. Azure App Service Environment (ASE) * B. Integration Service Environment (ISE) * C. VNet service endpoint   D. Azure AD B2B integration |
| Explanation | Scenario: The Shipping Logic App requires secure resources to the corporate VNet and use dedicated storage resources with a fixed costing model. You can access to Azure Virtual Network resources from Azure Logic Apps by using integration service environments (ISEs). Sometimes, your logic apps and integration accounts need access to secured resources, such as virtual machines (VMs) and other systems or services, that are inside an Azure virtual network. To set up this access, you can create an integration service environment (ISE) where you can run your logic apps and create your integration accounts. Reference: <https://docs.microsoft.com/en-us/azure/logic-apps/connect-virtual-network-vnet-isolated-environment-overview>  Implement Azure security |
| Question 6 | You need to resolve the Shipping web site error. How should you configre the Azure Table Storage service? |
| Answer |  |
| Explanation | Box 1: AllowedOrigins - A CORS request will fail if Access-Control-Allow-Origin is missing. Scenario: The following error message displays while you are testing the website:  Box 2: http://test-shippingapi.wideworldimporters.com Syntax: Access-Control-Allow-Origin: \* Access-Control-Allow-Origin: <origin> Access-Control-Allow-Origin: null <origin> Specifies an origin. Only a single origin can be specified.  Box 3: AllowedOrigins -  Box 4: POST - The only allowed methods are GET, HEAD, and POST. In this case POST is used. "<Corsrule>" "allowedmethods" Failed to load no "Access-control-Origin" header is present References: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Access-Control-Allow-Origin> |
| Question 7 | You need to migrate on-premises shipping data to Azure. What should you use? |
| Answer | * A. Azure Cosmos DB Data Migration tool (dt.exe) * B. Azure Database Migration service * C. AzCopy * D. Azure Migrate |
| Explanation | Migrate from on-premises or cloud implementations of MongoDB to Azure Cosmos DB with minimal downtime by using Azure Database Migration Service. Perform resilient migrations of MongoDB data at scale and with high reliability. Scenario: Data migration from on-premises to Azure must minimize costs and downtime. The application uses MongoDB JSON document storage database for all container and transport information. References: <https://azure.microsoft.com/en-us/updates/mongodb-to-azure-cosmos-db-online-and-offline-migrations-are-now-available/> |
| Question 8 | You need to support the message processing for the ocean transport workflow.  Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order. |
| Answer |  |
| Explanation | Step 1: Create an integration account in the Azure portal  You can define custom metadata for artifacts in integration accounts and get that metadata during runtime for your logic app to use. For example, you can provide metadata for artifacts, such as partners, agreements, schemas, and maps – all store metadata using key-value pairs.  Step 2: Link the Logic App to the integration account  A logic app that’s linked to the integration account and artifact metadata you want to use.  Step 3: Add partners, schemas, certificates, maps, and agreements  Step 4: Create a custom connector for the Logic App.  Reference: <https://docs.microsoft.com/bs-latn-ba/azure/logic-apps/logic-apps-enterprise-integration-metadata> |
| Question 9 | **You need to update the APIs to resolve the testing error.  How should you complete the Azure CLI command? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.** |
| Answer |  |
| Explanation | Cors add allowed-origins website |
| Question 10 | **You need to configure Azure App Service to support the REST API requirements.  Which values should you use?** |
| Answer |  |
| Explanation | Plan: Standard  Standard support auto-scaling  Instance Count: 10  Max instances for standard is 10.  Scenario:  The REST API’s that support the solution must meet the following requirements:  References: <https://azure.microsoft.com/en-us/pricing/details/app-service/plans/> |
| **Case** | **2** |
| Description | 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. 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:    Function app - RequestUserApproval.cs: |
| Question 1 | You need to correct the RequestUserApproval Function app error. What should you do? |
| Answer | **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. |
| 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" Reference: <https://docs.microsoft.com/en-us/azure/azure-functions/durable/durable-functions-http-features> |
| Question 2 | You need to configure the integration for Azure Service Bus and Azure Event Grid. How should you complete the CLI statement? To answer, select the appropriate options in the answer area. |
| Answer |  |
| Explanation | Box 1: eventgrid - To create event subscription use: az eventgrid event-subscription create  Box 2: event-subscription -  Box 3: servicebusqueue - Scenario: 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. Reference: https://docs.microsoft.com/en-us/cli/azure/eventgrid/event-subscription?view=azure-cli-latest#az\_eventgrid\_event\_subscription\_create Connect to and consume Azure services and third-party services |
| Question 3 | 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 |
| Answer |  |
| 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. 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>  Develop for Azure storage |
| Question 4 | You need to retrieve the database connection string. Which values should you use? To answer, select the appropriate options in the answer area. |
| Answer |  |
| 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 5 | 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. |
| 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 SCO5 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> |
| Question 6 | You need to configure API Management for authentication. Which policy values should you use? To answer, select the appropriate options in the answer area. |
| Answer |  |
| Explanation | Box 1: Validate JWT - The validate-jwt policy enforces existence and validity of a JWT extracted from either a specified HTTP Header or a specified query parameter. 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. Incorrect Answers: ✑ Limit call rate by key - Prevents API usage spikes by limiting call rate, on a per key basis. ✑ Restrict caller IPs - Filters (allows/denies) calls from specific IP addresses and/or address ranges. ✑ Check HTTP header - Enforces existence and/or value of a HTTP Header.  Box 2: Outbound - Reference: <https://docs.microsoft.com/en-us/azure/api-management/api-management-access-restriction-policies> |
| Question 7 | 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. |
| Answer | * A. ID token signature * B. ID token claims * C. HTTP response code * D. Azure AD endpoint URI * E. Azure AD tenant ID |
| Explanation | A: Claims in access tokens - JWTs (JSON Web Tokens) are split into three pieces: ✑ 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 Implement Azure security |
| Question 8 | You need to investigate the Azure Function app error message in the development environment. What should you do? |
| Answer | * 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. |
| 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>  Monitor, troubleshoot, and optimize Azure solutions |
| Question 9 | You need to ensure that all messages from Azure Event Grid are processed. What should you use? |
| Answer | * A. Azure Event Grid topic * B. Azure Service Bus topic * C. Azure Service Bus queue * D. Azure Storage queue * E. Azure Logic App custom connector |
| Explanation | As a solution architect/developer, you should consider using Service Bus queues when: ✑ Your solution needs to receive messages without having to poll the queue. With Service Bus, you can achieve it by using a long-polling receive operation using the TCP-based protocols that Service Bus supports. Reference: https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-azure-and-service-bus-queues-compared-contrasted Connect to and consume Azure services and third-party services |
| **Case** | **3** |
| Description | Background - You are a developer for Proseware, Inc. You are developing an application that applies a set of governance policies for Proseware"™s internal services, external services, and applications. The application will also provide a shared library for common functionality.  Requirements -  Policy service - You develop and deploy a stateful ASP.NET Core 2.1 web application named Policy service to an Azure App Service Web App. The application reacts to events from Azure Event Grid and performs policy actions based on those events. The application must include the Event Grid Event ID field in all Application Insights telemetry. Policy service must use Application Insights to automatically scale with the number of policy actions that it is performing.  Policies -  Log policy - All Azure App Service Web Apps must write logs to Azure Blob storage. All log files should be saved to a container named logdrop. Logs must remain in the container for 15 days.  Authentication events - Authentication events are used to monitor users signing in and signing out. All authentication events must be processed by Policy service. Sign outs must be processed as quickly as possible.  PolicyLib - You have a shared library named PolicyLib that contains functionality common to all ASP.NET Core web services and applications. The PolicyLib library must: Exclude non-user actions from Application Insights telemetry. Provide methods that allow a web service to scale itself. Ensure that scaling actions do not disrupt application usage.  Other -  Anomaly detection service - You have an anomaly detection service that analyzes log information for anomalies. It is implemented as an Azure Machine Learning model. The model is deployed as a web service. If an anomaly is detected, an Azure Function that emails administrators is called by using an HTTP WebHook.  Health monitoring - All web applications and services have health monitoring at the /health service endpoint.  Issues -  Policy loss - When you deploy Policy service, policies may not be applied if they were in the process of being applied during the deployment.  Performance issue - When under heavy load, the anomaly detection service undergoes slowdowns and rejects connections.  Notification latency - Users report that anomaly detection emails can sometimes arrive several minutes after an anomaly is detected.  App code -  EventGridController.cs - Relevant portions of the app files are shown below. Line numbers are included for reference only and include a two-character prefix that denotes the specific file to which they belong.    LoginEvent.cs - Relevant portions of the app files are shown below. Line numbers are included for reference only and include a two-character prefix that denotes the specific file to which they belong. |
| Question 1 | You need to resolve a notification latency issue. Which two actions should you perform? |
| Answer | **A.**Set Always On to true.  **B.**Ensure that the Azure Function is using an App Service plan.  **C.**Set Always On to false.  **D.**Ensure that the Azure Function is set to use a consumption plan. |
| Explanation | Azure Functions can run on either a Consumption Plan or a dedicated App Service Plan. If you run in a dedicated mode, you need to turn on the Always On setting for your Function App to run properly. The Function runtime will go idle after a few minutes of inactivity, so only HTTP triggers will actually "wake up" your functions. This is similar to how WebJobs must have Always On enabled. Scenario: Notification latency: Users report that anomaly detection emails can sometimes arrive several minutes after an anomaly is detected. Anomaly detection service: You have an anomaly detection service that analyzes log information for anomalies. It is implemented as an Azure Machine Learning model. The model is deployed as a web service. If an anomaly is detected, an Azure Function that emails administrators is called by using an HTTP WebHook. Reference: <https://github.com/Azure/Azure-Functions/wiki/Enable-Always-On-when-running-on-dedicated-App-Service-Plan> |
| Question 2 | You need to ensure that the solution can meet the scaling requirements for Policy Service. Which Azure Application Insights data model should you use? |
| Answer | * A. an Application Insights dependency * B. an Application Insights event * C. an Application Insights trace * D. an Application Insights metric |
| Explanation | Application Insights provides three additional data types for custom telemetry: Trace - used either directly, or through an adapter to implement diagnostics logging using an instrumentation framework that is familiar to you, such as Log4Net or System.Diagnostics. Event - typically used to capture user interaction with your service, to analyze usage patterns. Metric - used to report periodic scalar measurements. Scenario: Policy service must use Application Insights to automatically scale with the number of policy actions that it is performing. Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/app/data-model> |
| Question 3 | You need to meet the scaling requirements for Policy Service. What should you store in Azure Redis Cache? |
| Answer | * A. TempData * B. HttpContext.Items * C. ViewState * D. Session state |
| Explanation | Azure Cache for Redis provides a session state provider that you can use to store your session state in-memory with Azure Cache for Redis instead of a SQL Server database. Scenario: You have a shared library named PolicyLib that contains functionality common to all ASP.NET Core web services and applications. The PolicyLib library must: Ensure that scaling actions do not disrupt application usage. References: <https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-aspnet-session-state-provider> |
| Question 4 | How should you complete the Filter class? To answer, drag the appropriate code segments to the correct locations. Each code segment 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. |
| Answer |  |
| Explanation | Scenario: Exclude non-user actions from Application Insights telemetry.  Box 1: ITelemetryProcessor - To create a filter, implement ITelemetryProcessor. This technique gives you more direct control over what is included or excluded from the telemetry stream.  Box 2: ITelemetryProcessor -  Box 3: ITelemetryProcessor -  Box 4: RequestTelemetry -  Box 5: /health - To filter out an item, just terminate the chain. References: https://docs.microsoft.com/en-us/azure/azure-monitor/app/api-filtering-sampling |
| Question 5 | You need to implement the Log policy. How should you complete the Azure Event Grid subscription? To answer, drag the appropriate JSON segments to the correct locations. Each JSON segment 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 poin |
| Answer |  |
| Explanation | Box 1:WebHook - Scenario: If an anomaly is detected, an Azure Function that emails administrators is called by using an HTTP WebHook. endpointType: The type of endpoint for the subscription (webhook/HTTP, Event Hub, or queue).  Box 2: SubjectBeginsWith - Box 3: Microsoft.Storage.BlobCreated  Scenario: Log Policy - All Azure App Service Web Apps must write logs to Azure Blob storage. All log files should be saved to a container named logdrop. Logs must remain in the container for 15 days.  Example subscription schema - { "properties": { "destination": { "endpointType": "webhook", "properties": { "endpointUrl": "https://example.azurewebsites.net/api/HttpTriggerCSharp1?code=VXbGWce53l48Mt8wuotr0GPmyJ/nDT4hgdFj9DpBiRt38qqnnm5OFg==" } }, "filter": { "includedEventTypes": [ "Microsoft.Storage.BlobCreated", "Microsoft.Storage.BlobDeleted" ], "subjectBeginsWith": "blobServices/default/containers/mycontainer/log", [1] "isSubjectCaseSensitive ": "true" } } } References: https://docs.microsoft.com/en-us/azure/event-grid/subscription-creation-schema |
| Question 6 | You need to ensure that PolicyLib requirements are met. How should you complete the code segment? To answer, drag the appropriate code segments to the correct locations. Each code segment 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. |
| Answer |  |
| Explanation | Scenario: You have a shared library named PolicyLib that contains functionality common to all ASP.NET Core web services and applications. The PolicyLib library must: ✑ Exclude non-user actions from Application Insights telemetry. ✑ Provide methods that allow a web service to scale itself. ✑ Ensure that scaling actions do not disrupt application usage.  Box 1: ITelemetryInitializer - Use telemetry initializers to define global properties that are sent with all telemetry; and to override selected behavior of the standard telemetry modules.  Box 2: Initialize -  Box 3: Telemetry.Context - Box 4: [(EventTelemetry)telemetry.Properties("EventID") References: https://docs.microsoft.com/en-us/azure/azure-monitor/app/api-filtering-sampling |
| Question 7 | You need to implement the Log policy. How should you complete the EnsureLogging method in EventGridController.cs? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point. |
| Answer |  |
| Explanation | Box 1: logdrop - All log files should be saved to a container named logdrop.  Box 2: 15 - Logs must remain in the container for 15 days. Box 3: UpdateApplicationSettings All Azure App Service Web Apps must write logs to Azure Blob storage. References: https://blog.hompus.nl/2017/05/29/adding-application-logging-blob-to-a-azure-web-app-service-using-powershell/ |
| Question 8 | You need to ensure that authentication events are triggered and processed according to the authentication events policy. Solution: Ensure that signout events have a subject prefix. Create an Azure Event Grid subscription that uses the subjectBeginsWith filter. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | Scenario: Authentication events are used to monitor users signing in and signing out. All authentication events must be processed by Policy service. Sign outs must be processed as quickly as possible. References: https://docs.microsoft.com/en-us/azure/event-grid/subscription-creation-schema |
| Question 8 | You need to add code at line EG15 in EventGridController.cs to ensure that the Log policy applies to all services. How should you complete the code? To answer, drag the appropriate code segments to the correct locations. Each code segment 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. |
| Answer |  |
| Explanation | Scenario, Log policy: All Azure App Service Web Apps must write logs to Azure Blob storage.  Box 1: Status -  Box 2: Succeeded -  Box 3: operationName - Microsoft.Web/sites/write is resource provider operation. It creates a new Web App or updates an existing one. References: https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations |
| Question 9 | You need to insert code at line LE03 of LoginEvent.cs to ensure that all authentication events are procesed correctly. 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 |  |
| Explanation | Box 1: id - id is a unique identifier for the event.  Box 2: eventType - eventType is one of the registered event types for this event source.  Box 3: dataVersion - dataVersion is the schema version of the data object. The publisher defines the schema version. Scenario: Authentication events are used to monitor users signing in and signing out. All authentication events must be processed by Policy service. Sign outs must be processed as quickly as possible. The following example shows the properties that are used by all event publishers: [ { "topic": string, "subject": string, "id": string, "eventType": string, "eventTime": string, "data":{ object-unique-to-each-publisher }, "dataVersion": string, "metadataVersion": string } ] References: https://docs.microsoft.com/en-us/azure/event-grid/event-schema |
| Question 10 |  |
| Answer |  |
| Explanation |  |
| Question 11 |  |
| Answer |  |
| Explanation |  |
| **Case** | **4** |
| Description | Background -  Overview - You are a developer for Contoso, Ltd. The company has a social networking website that is developed as a Single Page Application (SPA). The main web application for the social networking website loads user uploaded content from blob storage. You are developing a solution to monitor uploaded data for inappropriate content. The following process occurs when users upload content by using the SPA: "¢ Messages are sent to ContentUploadService. "¢ Content is processed by ContentAnalysisService. "¢ After processing is complete, the content is posted to the social network or a rejection message is posted in its place. The ContentAnalysisService is deployed with Azure Container Instances from a private Azure Container Registry named contosoimages. The solution will use eight CPU cores.  Azure Active Directory - Contoso, Ltd. uses Azure Active Directory (Azure AD) for both internal and guest accounts.  Requirements -  ContentAnalysisService - The company's data science group built ContentAnalysisService which accepts user generated content as a string and returns a probable value for inappropriate content. Any values over a specific threshold must be reviewed by an employee of Contoso, Ltd. You must create an Azure Function named CheckUserContent to perform the content checks.  Costs - You must minimize costs for all Azure services.  Manual review - To review content, the user must authenticate to the website portion of the ContentAnalysisService using their Azure AD credentials. The website is built using React and all pages and API endpoints require authentication. In order to review content a user must be part of a ContentReviewer role. All completed reviews must include the reviewer's email address for auditing purposes.  High availability - All services must run in multiple regions. The failure of any service in a region must not impact overall application availability.  Monitoring - An alert must be raised if the ContentUploadService uses more than 80 percent of available CPU cores.  Security - You have the following security requirements: Any web service accessible over the Internet must be protected from cross site scripting attacks. All websites and services must use SSL from a valid root certificate authority. Azure Storage access keys must only be stored in memory and must be available only to the service. All Internal services must only be accessible from internal Virtual Networks (VNets). All parts of the system must support inbound and outbound traffic restrictions. All service calls must be authenticated by using Azure AD.  User agreements - When a user submits content, they must agree to a user agreement. The agreement allows employees of Contoso, Ltd. to review content, store cookies on user devices, and track user's IP addresses. Information regarding agreements is used by multiple divisions within Contoso, Ltd. User responses must not be lost and must be available to all parties regardless of individual service uptime. The volume of agreements is expected to be in the millions per hour.  Validation testing - When a new version of the ContentAnalysisService is available the previous seven days of content must be processed with the new version to verify that the new version does not significantly deviate from the old version.  Issues - Users of the ContentUploadService report that they occasionally see HTTP 502 responses on specific pages.  Code -  ContentUploadService - |
| Question | You need to configure the ContentUploadService deployment. Which two actions should you perform? Each correct answer presents part of the solution. |
| Answer | * A. Add the following markup to line CS23: type: Private * B. Add the following markup to line CS24: osType: Windows * C. Add the following markup to line CS24: osType: Linux * D. Add the following markup to line CS23: type: Public |
| Explanation | * Scenario: All Internal services must only be accessible from Internal Virtual Networks (VNets) There are three Network Location types "" Private, Public and Domain Reference: <https://devblogs.microsoft.com/powershell/setting-network-location-to-private/> |
| Question 2 | * You need to store the user agreements. Where should you store the agreement after it is completed? |
| Answer | * A. Azure Storage queue * B. Azure Event Hub * C. Azure Service Bus topic * D. Azure Event Grid topic |
| Explanation | * Azure Event Hub is used for telemetry and distributed data streaming. This service provides a single solution that enables rapid data retrieval for real-time processing as well as repeated replay of stored raw data. It can capture the streaming data into a file for processing and analysis. It has the following characteristics: low latency capable of receiving and processing millions of events per second at least once delivery Reference: <https://docs.microsoft.com/en-us/azure/event-grid/compare-messaging-services> |
| Question 3 | * You need to implement the bindings for the CheckUserContent function. How should you complete the code segment? To answer, select the appropriate options in the answer area. |
| Answer |  |
| Explanation | Box 1: [BlobTrigger(..)] Box 2: [Blob(..)] Azure Blob storage output binding for Azure Functions. The output binding allows you to modify and delete blob storage data in an Azure Function. The attribute's constructor takes the path to the blob and a FileAccess parameter indicating read or write, as shown in the following example: [FunctionName("ResizeImage")] public static void Run( [BlobTrigger("sample-images/{name}")] Stream image, [Blob("sample-images-md/{name}", FileAccess.Write)] Stream imageSmall) { ... } Scenario: You must create an Azure Function named CheckUserContent to perform the content checks. The company's data science group built ContentAnalysisService which accepts user generated content as a string and returns a probable value for inappropriate content. Any values over a specific threshold must be reviewed by an employee of Contoso, Ltd. Reference: <https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-storage-blob-output>  Develop for Azure storage |
| Question 4 | * You need to add markup at line AM04 to implement the ContentReview role. How should you complete the markup? To answer, drag the appropriate json segments to the correct locations. Each json segment 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. |
| Answer |  |
| Explanation | Box 1: allowedMemberTypes - allowedMemberTypes specifies whether this app role definition can be assigned to users and groups by setting to "User", or to other applications (that are accessing this application in daemon service scenarios) by setting to "Application", or to both. Note: The following example shows the appRoles that you can assign to users. "appId": "8763f1c4-f988-489c-a51e-158e9ef97d6a", "appRoles": [ { "allowedMemberTypes": [ "User" ], "displayName": "Writer", "id": "d1c2ade8-98f8-45fd-aa4a-6d06b947c66f", "isEnabled": true, "description": "Writers Have the ability to create tasks.", "value": "Writer" } ], "availableToOtherTenants": false,  Box 2: User - Scenario: In order to review content a user must be part of a ContentReviewer role.  Box 3: value - value specifies the value which will be included in the roles claim in authentication and access tokens. Reference: <https://docs.microsoft.com/en-us/graph/api/resources/approle> |
| Question 5 | * You need to add code at line AM09 to ensure that users can review content using ContentAnalysisService. How should you complete the code? To answer, select the appropriate options in the answer area |
| Answer |  |
| Explanation | * Box 1: "oauth2Permissions": ["login"] oauth2Permissions specifies the collection of OAuth 2.0 permission scopes that the web API (resource) app exposes to client apps. These permission scopes may be granted to client apps during consent. Box 2: "oauth2AllowImplicitFlow":true For applications (Angular, Ember.js, React.js, and so on), Microsoft identity platform supports the OAuth 2.0 Implicit Grant flow. Reference: <https://docs.microsoft.com/en-us/azure/active-directory/develop/reference-app-manifest> |
| Question 6 | * 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. |
| Answer |  |
| Explanation | 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>  Implement Azure security |
| Question 7 | * You need to monitor ContentUploadService according to the requirements. Which command should you use? |
| Answer | * A. az monitor metrics alert create ""n alert ""g "¦ - -scopes "¦ - -condition "avg Percentage CPU > 8" * B. az monitor metrics alert create ""n alert ""g "¦ - -scopes "¦ - -condition "avg Percentage CPU > 800" * C. az monitor metrics alert create ""n alert ""g "¦ - -scopes "¦ - -condition "CPU Usage > 800" * D. az monitor metrics alert create ""n alert ""g "¦ - -scopes "¦ - -condition "CPU Usage > 8" |
| Explanation | * Scenario: An alert must be raised if the ContentUploadService uses more than 80 percent of available CPU cores Reference: <https://docs.microsoft.com/sv-se/cli/azure/monitor/metrics/alert>  Monitor, troubleshoot, and optimize Azure solutions |
| **Case** | * **5** |
| Description | * Background - You are a developer for Litware Inc., a SaaS company that provides a solution for managing employee expenses. The solution consists of an ASP.NET Core Web API project that is deployed as an Azure Web App.  Overall architecture - Employees upload receipts for the system to process. When processing is complete, the employee receives a summary report email that details the processing results. Employees then use a web application to manage their receipts and perform any additional tasks needed for reimbursement.  Receipt processing - Employees may upload receipts in two ways: Uploading using an Azure Files mounted folder Uploading using the web application  Data Storage - Receipt and employee information is stored in an Azure SQL database.  Documentation - Employees are provided with a getting started document when they first use the solution. The documentation includes details on supported operating systems for Azure File upload, and instructions on how to configure the mounted folder.  Solution details -  Users table -   Web Application - You enable MSI for the Web App and configure the Web App to use the security principal name.  Processing - Processing is performed by an Azure Function that uses version 2 of the Azure Function runtime. Once processing is completed, results are stored in Azure Blob Storage and an Azure SQL database. Then, an email summary is sent to the user with a link to the processing report. The link to the report must remain valid if the email is forwarded to another user.  Requirements -  Receipt processing - Concurrent processing of a receipt must be prevented.  Logging - Azure Application Insights is used for telemetry and logging in both the processor and the web application. The processor also has TraceWriter logging enabled. Application Insights must always contain all log messages.  Disaster recovery - Regional outage must not impact application availability. All DR operations must not be dependent on application running and must ensure that data in the DR region is up to date.  Security - Users' SecurityPin must be stored in such a way that access to the database does not allow the viewing of SecurityPins. The web application is the only system that should have access to SecurityPins. All certificates and secrets used to secure data must be stored in Azure Key Vault. You must adhere to the Least Privilege Principal and provide privileges which are essential to perform the intended function. All access to Azure Storage and Azure SQL database must use the application's Managed Service Identity (MSI) Receipt data must always be encrypted at rest. All data must be protected in transit. User's expense account number must be visible only to logged in users. All other views of the expense account number should include only the last segment with the remaining parts obscured. In the case of a security breach, access to all summary reports must be revoked without impacting other parts of the system.  Issues -  Upload format issue - Employees occasionally report an issue with uploading a receipt using the web application. They report that when they upload a receipt using the Azure File Share, the receipt does not appear in their profile. When this occurs, they delete the file in the file share and use the web application, which returns a 500 Internal Server error page.  Capacity issue - During busy periods, employees report long delays between the time they upload the receipt and when it appears in the web application.  Log capacity issue - Developers report that the number of log messages in the trace output for the processor is too high, resulting in lost log messages.  Processing.cs -   Database.cs -   ReceiptUploader.cs -   ConfigureSSE.ps1 - |
| Question 1 | * You need to ensure that security requirements are met. What value should be used for the ConnectionString field on line DB03 in the Database class? |
| Answer |  |
| Explanation | Box 1: Integrated Security=SSPI - Integrated security: For all data source types, connect using the current user account. For SqlClient you can use Integrated Security=true; or Integrated Security=SSPI; Scenario: All access to Azure Storage and Azure SQL database must use the application's Managed Service Identity (MSI)  Box 2: Encrypt = True - Scenario: All data must be protected in transit. References: <https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax> |
| Question 2 | * You need to ensure disaster recovery requirements are met. What code should you add at line PC16? To answer, drag the appropriate code fragments to the correct locations. Each code fragment 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. |
| Answer |  |
| Explanation | * Scenario: Disaster recovery. Regional outage must not impact application availability. All DR operations must not be dependent on application running and must ensure that data in the DR region is up to date.  Box 1: DirectoryTransferContext - We transfer all files in the directory. Note: The TransferContext object comes in two forms: SingleTransferContext and DirectoryTransferContext. The former is for transferring a single file and the latter is for transferring a directory of files. Box 2: ShouldTransferCallbackAsync The DirectoryTransferContext.ShouldTransferCallbackAsync delegate callback is invoked to tell whether a transfer should be done.  Box 3: False - If you want to use the retry policy in Copy, and want the copy can be resume if break in the middle, you can use SyncCopy (isServiceCopy = false). Note that if you choose to use service side copy ('isServiceCopy' set to true), Azure (currently) doesn't provide SLA for that. Setting 'isServiceCopy' to false will download the source blob loca References: https://docs.microsoft.com/en-us/azure/storage/common/storage-use-data-movement-library https://docs.microsoft.com/en-us/dotnet/api/microsoft.windowsazure.storage.datamovement.directorytransfercontext.shouldtransfercallbackasync?view=azure- dotnet |
| Question 2 | * You need to ensure the security policies are met. What code do you add at line CS07? |
| Answer | * A. -PermissionsToCertificates create, encrypt, decrypt * B. -PermissionsToKeys wrapkey, unwrapkey, get * C. -PermissionsToCertificates wrapkey, unwrapkey, get * D. -PermissionsToKeys create, encrypt, decrypt |
| Explanation | * Scenario: All certificates and secrets used to secure data must be stored in Azure Key Vault. You must adhere to the principle of least privilege and provide privileges which are essential to perform the intended function. The Set-AzureRmKeyValutAccessPolicy parameter -PermissionsToKeys specifies an array of key operation permissions to grant to a user or service principal. The acceptable values for this parameter: decrypt, encrypt, unwrapKey, wrapKey, verify, sign, get, list, update, create, import, delete, backup, restore, recover, purge Incorrect Answers: A, C: The Set-AzureRmKeyValutAccessPolicy parameter -PermissionsToCertificates specifies an array of certificate permissions to grant to a user or service principal. The acceptable values for this parameter: get, list, delete, create, import, update, managecontacts, getissuers, listissuers, setissuers, deleteissuers, manageissuers, recover, purge, backup, restore References: <https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurermkeyvaultaccesspolicy> |
| Question 3 | * You need to ensure that the SecurityPin security requirements are met. Solution: Enable Always Encrypted for the SecurityPin column using a certificate contained in Azure Key Vault and grant the WebAppIdentity service principal access to the certificate. Does the solution meet the goal? |
| Answer | * Yes |
| Explanation | * Scenario: Users' SecurityPin must be stored in such a way that access to the database does not allow the viewing of SecurityPins. The web application is the only system that should have access to SecurityPins. |
| Question 4 | * You need to ensure that the SecurityPin security requirements are met. Solution: Configure the web application to connect to the database using the WebAppIdentity security prinicipal. Using the Azure Portal, add Data Masking to the SecurityPin column and exclude the WebAppIdentity service principal. Does the solution meet the goal? |
| Answer | * Yes |
| Explanation | * Scenario: Users' SecurityPin must be stored in such a way that access to the database does not allow the viewing of SecurityPins. The web application is the only system that should have access to SecurityPins. All certificates and secrets used to secure data must be stored in Azure Key Vault. |
| Question 4 | * Solution: Enable Always Encrypted for the SecurityPin column using a certificate based on a trusted certificate authority. Update the Getting Started document with instructions to ensure that the certificate is installed on user machines. Does the solution meet the goal? |
| Answer | * No |
| Explanation | * Scenario: Users' SecurityPin must be stored in such a way that access to the database does not allow the viewing of SecurityPins. The web application is the only system that should have access to SecurityPins. All certificates and secrets used to secure data must be stored in Azure Key Vault. |
| Question 5 | * You need to ensure that security policies are met. What code should you add at line PC26? |
| Answer |  |
| Explanation | * Box 1: var key = await Resolver.ResolveKeyAsyn(keyBundle,KeyIdentifier.CancellationToken.None); Box 2: var x = new BlobEncryptionPolicy(key,resolver); Example: // We begin with cloudKey1, and a resolver capable of resolving and caching Key Vault secrets. BlobEncryptionPolicy encryptionPolicy = new BlobEncryptionPolicy(cloudKey1, cachingResolver); client.DefaultRequestOptions.EncryptionPolicy = encryptionPolicy; Box 3: cloudblobClient. DefaultRequestOptions.EncryptionPolicy = x; References: <https://github.com/Azure/azure-storage-net/blob/master/Samples/GettingStarted/EncryptionSamples/KeyRotation/Program.cs> |
| Question 6 | * You need to ensure that security requirements are met. How should you complete the code segment? |
| Answer |  |
| Explanation | * **Correct Answer:** *Explanation* Box 1: ExpenseAccount - Scenario: User's expense account number must be visible only to logged in users. All other views of the expense account number should include only the last segment. With the remaining parts obscured.  Box 2: Text - If MaskingFunction has a value of Number or Text, you can specify the NumberFrom and NumberTo parameters, for number masking, or the PrefixSize, ReplacementString, and SuffixSize for text masking.  Box 3: 4 - -SuffixSize specifies the number of characters at the end of the text that are not masked. Specify this parameter only if you specify a value of Text for the MaskingFunction parameter. Scenario: Format is 1234-1234-1235 Box 4: xxxx" Scenario: Format is 1234-1234-1235 References: https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/new-azurermsqldatabasedatamaskingrule?view=azurermps-6.13.0 |
| Question 7 | * You need to ensure that authentication events are triggered and processed according to the authentication events policy. Solution: Create a new Azure Event Grid subscription for all authentication that delivers messages to an Azure Event Hub. Use the subscription to process signout events. Does the solution meet the goal? |
| Answer | * No |
| Explanation | * Use a separate Azure Event Grid topics and subscriptions for sign-in and sign-out events. Scenario: Authentication events are used to monitor users signing in and signing out. All authentication events must be processed by Policy service. Sign outs must be processed as quickly as possible. |
| Question 8 | You need to ensure that authentication events are triggered and processed according to the authentication events policy.  Solution: Create separate Azure Event Grid topics and subscriptions for sign-in and sign-out events.   * Does the solution meet the goal? |
| Answer | * Yes/No |
| Explanation | * Instead ensure that signout events have a subject prefix. Create an Azure Event Grid subscription that uses the subjectBeginsWith filter. Scenario: Authentication events are used to monitor users signing in and signing out. All authentication events must be processed by Policy service. Sign outs must be processed as quickly as possible. |
| Question 9 | * You need to resolve the log capacity issue. What should you do? |
| Answer | * A. Set a LogCategoryFilter during startup. * B. Create an Application Insights Telemetry Filter. * C. Change the minimum log level in the host.json file for the function. * D. Implement Application Insights Sampling. |
| Explanation | * Scenario, the log capacity issue: Developers report that the number of log message in the trace output for the processor is too high, resulting in lost log messages. Sampling is a feature in Azure Application Insights. It is the recommended way to reduce telemetry traffic and storage, while preserving a statistically correct analysis of application data. The filter selects items that are related, so that you can navigate between items when you are doing diagnostic investigations. When metric counts are presented to you in the portal, they are renormalized to take account of the sampling, to minimize any effect on the statistics. Sampling reduces traffic and data costs, and helps you avoid throttling. References: <https://docs.microsoft.com/en-us/azure/azure-monitor/app/sampling> |
| Question 10 | * You need to resolve the capacity issue. What should you do? |
| Answer | * A. Move the Azure Function to a dedicated App Service Plan. * B. Convert the trigger on the Azure Function to a File Trigger. * C. Ensure that the consumption plan is configured correctly to allow for scaling. * D. Update the loop starting on line PC09 to process items in parallel. |
| Explanation | * If you want to read the files in parallel, you cannot use forEach. Each of the async callback function calls does return a promise. You can await the array of promises that you'll get with Promise.all. Scenario: Capacity issue: During busy periods, employees report long delays between the time they upload the receipt and when it appears in the web application.  References: https://stackoverflow.com/questions/37576685/using-async-await-with-a-foreach-loop |
| Question 11 | * You need to ensure receipt processing occurs correctly. What should you do? |
| Answer | * A. Use blob metadata to prevent concurrency problems. * B. Use blob SnapshotTime to prevent concurrency problems. * C. Use blob leases to prevent concurrency problems. * D. Use blob properties to prevent concurrency problems. |
| Explanation | * You can create a snapshot of a blob. A snapshot is a read-only version of a blob that's taken at a point in time. Once a snapshot has been created, it can be read, copied, or deleted, but not modified. Snapshots provide a way to back up a blob as it appears at a moment in time. Scenario: Processing is performed by an Azure Function that uses version 2 of the Azure Function runtime. Once processing is completed, results are stored in Azure Blob Storage and an Azure SQL database. Then, an email summary is sent to the user with a link to the processing report. The link to the report must remain valid if the email is forwarded to another user. References: <https://docs.microsoft.com/en-us/rest/api/storageservices/creating-a-snapshot-of-a-blob> |
| Question 12 | * You need to configure retries in the LoadUserDetails function in the Database class without impacting user experience. What code should you insert on line DB07? To answer, select the appropriate options in the answer area. |
| Answer |  |
| Explanation | * Box 1: Policy -  RetryPolicy retry = Policy - .Handle<HttpRequestException>() .Retry(3); The above example will create a retry policy which will retry up to three times if an action fails with an exception handled by the Policy. Box 2: WaitAndRetryAsync(3,i => TimeSpan.FromMilliseconds(100\* Math.Pow(2,i-1))); A common retry strategy is exponential backoff: this allows for retries to be made initially quickly, but then at progressively longer intervals, to avoid hitting a subsystem with repeated frequent calls if the subsystem may be struggling. Example:  Policy - .Handle<SomeExceptionType>() .WaitAndRetry(3, retryAttempt => TimeSpan.FromSeconds(Math.Pow(2, retryAttempt)) ); References: <https://github.com/App-vNext/Polly/wiki/Retry> |
| Question 13 | * You need to add code at line PC32 in Processing.cs to implement the GetCredentials method in the Processing class. How should you complete the code? To answer, drag the appropriate code segments to the correct locations. Each code segment 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. |
| Answer |  |
| Explanation | Box 1: AzureServiceTokenProvider() Box 2: tp.GetAccessTokenAsync("..") Acquiring an access token is then quite easy. Example code: private async Task<string> GetAccessTokenAsync() { var tokenProvider = new AzureServiceTokenProvider(); return await tokenProvider.GetAccessTokenAsync("https://storage.azure.com/"); } References: <https://joonasw.net/view/azure-ad-authentication-with-azure-storage-and-managed-service-identity> |
| Question 14 | You need to construct the link to the summary report for the email that is sent to users. What should you do? |
| Answer | * A. Create a SharedAccessBlobPolicy and add it to the containers SharedAccessPolicies. Call GetSharedAccessSignature on the blob and use the resulting link. * B. Create a SharedAccessAccountPolicy and call GetSharedAccessSignature on storage account and use the resulting link. * C. Create a SharedAccessBlobPolicy and set the expiry time to two weeks from today. Call GetSharedAccessSignature on the blob and use the resulting link. * D. Create a SharedAccessBlobPolicy and set the expiry time to two weeks from today. Call GetSharedAccessSignature on the container and use the resulting link. |
| Explanation | Scenario: Processing is performed by an Azure Function that uses version 2 of the Azure Function runtime. Once processing is completed, results are stored in Azure Blob Storage and an Azure SQL database. Then, an email summary is sent to the user with a link to the processing report. The link to the report must remain valid if the email is forwarded to another user. Create a stored access policy to manage signatures on a container's resources, and then generate the shared access signature on the container, setting the constraints directly on the signature. Code example: Add a method that generates the shared access signature for the container and returns the signature URI. static string GetContainerSasUri(CloudBlobContainer container) { //Set the expiry time and permissions for the container. //In this case no start time is specified, so the shared access signature becomes valid immediately. SharedAccessBlobPolicy sasConstraints = new SharedAccessBlobPolicy(); sasConstraints.SharedAccessExpiryTime = DateTimeOffset.UtcNow.AddHours(24); sasConstraints.Permissions = SharedAccessBlobPermissions.List | SharedAccessBlobPermissions.Write; //Generate the shared access signature on the container, setting the constraints directly on the signature. string sasContainerToken = container.GetSharedAccessSignature(sasConstraints); //Return the URI string for the container, including the SAS token. return container.Uri + sasContainerToken; } Incorrect Answers: C: Call GetSharedAccessSignature on the container, not on the blob. References: <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-dotnet-shared-access-signature-part-2> |
| Question 15 | You need to ensure that security requirements are met. What value should be used for the ConnectionString field on line DB03 in the Database class? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point. |
| Answer |  |
| Explanation | Box 1: Integrated Security=SSPI - Integrated security: For all data source types, connect using the current user account. For SqlClient you can use Integrated Security=true; or Integrated Security=SSPI; Scenario: All access to Azure Storage and Azure SQL database must use the application's Managed Service Identity (MSI)  Box 2: Encrypt = True - Scenario: All data must be protected in transit. References: <https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax> |
| Question 16 | You need to ensure that the upload format issue is resolved. What code should you add at line RU14? To answer, drag the appropriate code fragments to the correct locations. Each code segment 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. |
| Answer |  |
| Explanation | Box 1: HttpStatusCode.InternalServerError Box 2: CannotDeleteFileOrDirectory  Scenario: Upload format issue - Employees occasionally report an issue with uploading a receipt using the web application. They report that when they upload a receipt using the Azure File Share, the receipt does not appear in their profile. When this occurs, they delete the file in the file share and use the web application, which returns a 500 Internal Server error page. |
| **Case** | * **6** |
| Description | * LabelMaker app - Coho Winery produces bottles, and distributes a variety of wines globally. You are developer implementing highly scalable and resilient applications to support online order processing by using Azure solutions. Coho Winery has a LabelMaker application that prints labels for wine bottles. The application sends data to several printers. The application consists of five modules that run independently on virtual machines (VMs). Coho Winery plans to move the application to Azure and continue to support label creation. External partners send data to the LabelMaker application to include artwork and text for custom label designs.  Data - You identify the following requirements for data management and manipulation: Order data is stored as nonrelational JSON and must be queried using Structured Query Language (SQL). Changes to the Order data must reflect immediately across all partitions. All reads to the Order data must fetch the most recent writes. You have the following security requirements: Users of Coho Winery applications must be able to provide access to documents, resources, and applications to external partners. External partners must use their own credentials and authenticate with their organization's identity management solution. External partner logins must be audited monthly for application use by a user account administrator to maintain company compliance.  Storage of e-commerce application settings must be maintained in Azure Key Vault. E-commerce application sign-ins must be secured by using Azure App Service authentication and Azure Active Directory (AAD). Conditional access policies must be applied at the application level to protect company content The LabelMaker applications must be secured by using an AAD account that has full access to all namespaces of the Azure Kubernetes Service (AKS) cluster.  LabelMaker app - Azure Monitor Container Health must be used to monitor the performance of workloads that are deployed to Kubernetes environments and hosted on Azure Kubernetes Service (AKS). You must use Azure Container Registry to publish images that support the AKS deployment.  Calls to the Printer API App fail periodically due to printer communication timeouts. Printer communications timeouts occur after 10 seconds. The label printer must only receive up to 5 attempts within one minute. The order workflow fails to run upon initial deployment to Azure.  Order .json - |
| Question 1 | * You need to troubleshoot the order workflow. What should you do? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point. |
| Answer | * A. Review the trigger history. * B. Review the API connections. * C. Review the run history. * D. Review the activity log. |
| Explanation | * Scenario: The order workflow fails to run upon initial deployment to Azure. Deployment errors arise from conditions that occur during the deployment process. They appear in the activity log. References: https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-audit |
| Question 2 | * You need to ensure that you can deploy the LabelMaker application. How should you complete the CLI commands? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point. |
| Answer |  |
| Explanation | * Box 1: group - Create a resource group with the az group create command. An Azure resource group is a logical group in which Azure resources are deployed and managed. The following example creates a resource group named myResourceGroup in the westeurope location. az group create --name myResourceGroup --location westeurope  Box 2: CohoWinterLabelMaker - Use the resource group named, which is used in the second command.  Box 3: aks - The command az aks create, is used to create a new managed Kubernetes cluster.  Box 4: monitoring -  Scenario: LabelMaker app - Azure Monitor Container Health must be used to monitor the performance of workloads that are deployed to Kubernetes environments and hosted on Azure Kubernetes Service (AKS). You must use Azure Container Registry to publish images that support the AKS deployment. |
| Question 3 | * You need to implement the e-commerce checkout API. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point. |
| Answer | * A. Set the function template's Mode property to Webhook and the Webhook type property to Generic JSON. * B. Create an Azure Function using the HTTP POST function template. * C. In the Azure Function App, enable Cross-Origin Resource Sharing (CORS) with all origins permitted. * D. In the Azure Function App, enable Managed Service Identity (MSI). * E. Set the function template's Mode property to Webhook and the Webhook type property to GitHub. * F. Create an Azure Function using the Generic webhook function template. |
| Explanation | * Scenario: E-commerce application sign-ins must be secured by using Azure App Service authentication and Azure Active Directory (AAD). D: A managed identity from Azure Active Directory allows your app to easily access other AAD-protected resources such as Azure Key Vault. Incorrect Answers: C: CORS is an HTTP feature that enables a web application running under one domain to access resources in another domain. References: https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity |
| Question 4 | * You need to deploy a new version of the LabelMaker application. 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. |
| Answer |  |
| Explanation | * Step 1: Build a new application image by using dockerfile Step 2: Create an alias if the image with the fully qualified path to the registry Before you can push the image to a private registry, you've to ensure a proper image name. This can be achieved using the docker tag command. For demonstration purpose, we'll use Docker's hello world image, rename it and push it to ACR. # pulls hello-world from the public docker hub $ docker pull hello-world # tag the image in order to be able to push it to a private registry $ docker tag hello-word <REGISTRY\_NAME>/hello-world # push the image $ docker push <REGISTRY\_NAME>/hello-world Step 3: Log in to the registry and push image In order to push images to the newly created ACR instance, you need to login to ACR form the Docker CLI. Once logged in, you can push any existing docker image to your ACR instance. Scenario: Coho Winery plans to move the application to Azure and continue to support label creation.  LabelMaker app - Azure Monitor Container Health must be used to monitor the performance of workloads that are deployed to Kubernetes environments and hosted on Azure Kubernetes Service (AKS). You must use Azure Container Registry to publish images that support the AKS deployment. References: https://thorsten-hans.com/how-to-use-a-private-azure-container-registry-with-kubernetes-9b86e67b93b6 https://docs.microsoft.com/en-us/azure/container-registry/container-registry-tutorial-quick-task |
| Question 5 | * You need to provision and deploy the order workflow. Which three components should you include? |
| Answer | * A. Connections * B. On-premises Data Gateway * C. Workflow definition * D. Resources * E. Functions |
| Explanation |  |
| Question 6 | * You need to update the order workflow to address the issue when calling the Printer API App. How should you complete the code? To answer, select the appropriate options in the answer area. |
| Answer |  |
| Explanation | Box 1: Fixed - To specify that the action or trigger waits the specified interval before sending the next request, set the <retry-policy-type> to fixed.  Box 2: PT10S -  Box 3: 5 - Scenario: Calls to the Printer API App fail periodically due to printer communication timeouts. Printer communication timeouts occur after 10 seconds. The label printer must only receive up to 5 attempts within one minute. Incorrect Answers: Default: If you don't specify a retry policy, the action uses the default policy, which is actually an exponential interval policy that sends up to four retries at exponentially increasing intervals that are scaled by 7.5 seconds. The interval is capped between 5 and 45 seconds. References: <https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-exception-handling> |
| Question 7 | * You need to retrieve all order line items sorted alphabetically by the city. How should you complete the code? |
| Answer |  |
| Explanation | * Order data is stored as nonrelational JSON and must be queried using Structured Query Language (SQL). The Order data is stored in a Cosmos database. |
| Question 8 | * You need to configure Azure Cosmos DB. Which settings should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point |
| Answer |  |
| Explanation | * Box 1: Strong - When the consistency level is set to strong, the staleness window is equivalent to zero, and the clients are guaranteed to read the latest committed value of the write operation. Scenario: Changes to the Order data must reflect immediately across all partitions. All reads to the Order data must fetch the most recent writes. Note: You can choose from five well-defined models on the consistency spectrum. From strongest to weakest, the models are: Strong, Bounded staleness, Session, Consistent prefix, Eventual  Box 2: SQL - Scenario: You identify the following requirements for data management and manipulation: Order data is stored as nonrelational JSON and must be queried using Structured Query Language (SQL). |
| Question 9 | * You need to meet the security requirements for external partners. Which Azure Active Directory features should you use? |
| Answer |  |
| Explanation | * Box 1: B2B - Scenario: External partners must use their own credentials and authenticate with their organization's identity management solution. Azure Active Directory (Azure AD) business-to-business (B2B) collaboration lets you securely share your company's applications and services with guest users from any other organization, while maintaining control over your own corporate data. Work safely and securely with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources. Developers can use Azure AD business-to-business APIs to customize the invitation process or write applications like self-service sign-up portals.  Box 2: Access Review - Scenario: External partner logins must be audited monthly for application use by a user account administrator to maintain company compliance. Azure Active Directory (Azure AD) Access Reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. Administrators can use Azure Active Directory (Azure AD) to create an access review for group members or users assigned to an application. Azure AD automatically sends reviewers an email that prompts them to review access. References: <https://docs.microsoft.com/en-us/azure/active-directory/b2b/what-is-b2b> |
| Question 10 | * You need to meet the security requirements for the E-Commerce Web App. Which two steps should you take? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point. |
| Answer | * A. Update the E-Commerce Web App with the service principal's client secret. * B. Enable Managed Service Identity (MSI) on the E-Commerce Web App. * C. Add a policy to the Azure Key Vault to grant access to the E-Commerce Web App. * D. Create an Azure AD service principal. |
| Explanation | * Scenario: E-commerce application sign-ins must be secured by using Azure App Service authentication and Azure Active Directory (AAD). A managed identity from Azure Active Directory allows your app to easily access other AAD-protected resources such as Azure Key Vault. T References: <https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity> |
| Question 11 | You need to access user claims in the e-commerce web app. What should you do first? |
| Answer | * A. Using the Azure CLI, enable Cross-origin resource sharing (CORS) from the e-commerce checkout API to the e-commerce web app. * B. Update the e-commerce web app to read the HTTP request header values. * C. Assign the Contributor RBAC role to the e-commerce web app by using the Resource Manager create role assignment API. * D. Write custom code to make a Microsoft Graph API call from the e-commerce web app. |
| Explanation | * If you want more information about the user, you'll need to use the Azure AD Graph API. References: https://docs.microsoft.com/en-us/azure/architecture/multitenant-identity/claims |
| Question 12 | * You need to meet the LabelMaker application security requirement. What should you do? |
| Answer | * A. Create a conditional access policy and assign it to the Azure Kubernetes Service cluster. * B. Place the Azure Active Directory account into an Azure AD group. Create a ClusterRoleBinding and assign it to the group. * C. Create a RoleBinding and assign it to the Azure AD account. * D. Create a Microsoft Azure Active Directory service principal and assign it to the Azure Kubernetes Service (AKS) cluster. |
| Explanation | * Scenario: The LabelMaker applications must be secured by using an AAD account that has full access to all namespaces of the Azure Kubernetes Service (AKS) cluster. Permissions can be granted within a namespace with a RoleBinding, or cluster-wide with a ClusterRoleBinding. References: https://kubernetes.io/docs/reference/access-authn-authz/rbac/ |
| Question 13 | You need to meet the LabelMaker application security requirement. Solution: Create a Microsoft Azure Active Directory service principal and assign it to the Azure Kubernetes Service (AKS) cluster. Does the solution meet the goal? |
| Answer | * No |
| Explanation | * Scenario: The LabelMaker applications must be secured by using an AAD account that has full access to all namespaces of the Azure Kubernetes Service (AKS) cluster. Permissions can be granted within a namespace with a RoleBinding, or cluster-wide with a ClusterRoleBinding. References: https://kubernetes.io/docs/reference/access-authn-authz/rbac/ |
| Question 14 | * You need to meet the LabelMaker application security requirement. Solution: Create a RoleBinding and assign it to the Azure AD account. Does the solution meet the goal? |
| Answer | * No |
| Explanation | * We would need a ClusterRoleBinding. A correction solution would be: Place the Azure Active Directory account into an Azure AD group. Create a ClusterRoleBinding and assign it to the group. Scenario: The LabelMaker applications must be secured by using an AAD account that has full access to all namespaces of the Azure Kubernetes Service (AKS) cluster. Permissions can be granted within a namespace with a RoleBinding, or cluster-wide with a ClusterRoleBinding. References: <https://kubernetes.io/docs/reference/access-authn-authz/rbac/> |
| Question 15 | * You need to meet the LabelMaker application security requirement. Solution: Create a conditional access policy and assign it to the Azure Kubernetes Service cluster. Does the solution meet the goal? |
| Answer | * No |
| Explanation | * Scenario: The LabelMaker applications must be secured by using an AAD account that has full access to all namespaces of the Azure Kubernetes Service (AKS) cluster. Before an Azure Active Directory account can be used with the AKS cluster, a role binding or cluster role binding needs to be created. References: https://docs.microsoft.com/en-us/azure/aks/aad-integration |
|  |  |
|  |  |
|  |  |