|  |  |
| --- | --- |
| Scenario | You develop a software as a service (SaaS) offering to manage photographs. Users upload photos to a web service which then stores the photos in Azure Storage Blob storage. The storage account type is General-purpose V2. When photos are uploaded, they must be processed to produce and save a mobile-friendly version of the image. The process to produce a mobile-friendly version of the image must start in less than one minute. You need to design the process that starts the photo processing. Solution: Trigger the photo processing from Blob storage events. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | You need to catch the triggered event, so move the photo processing to an Azure Function triggered from the blob upload Note: Azure Storage events allow applications to react to events. Common Blob storage event scenarios include image or video processing, search indexing, or any file-oriented workflow. Events are pushed using Azure Event Grid to subscribers such as Azure Functions, Azure Logic Apps, or even to your own http listener. Note: Only storage accounts of kind StorageV2 (general purpose v2) and BlobStorage support event integration. Storage (general purpose v1) does not support integration with Event Grid. Reference: <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-event-overview> |
| Scenario | You develop and deploy an Azure App Service API app to a Windows-hosted deployment slot named Development. You create additional deployment slots named Testing and Production. You enable auto swap on the Production deployment slot. You need to ensure that scripts run and resources are available before a swap operation occurs. Solution: Update the web.config file to include the applicationInitialization configuration element. Specify custom initialization actions to run the scripts. Does the solution meet the goal? |
| Answer | No |
| Explanation | Specify custom warm-up. Some apps might require custom warm-up actions before the swap. The applicationInitialization configuration element in web.config lets you specify custom initialization actions. The swap operation waits for this custom warm-up to finish before swapping with the target slot. Here's a sample web.config fragment. <system.webServer> <applicationInitialization> <add initializationPage="/" hostName="[app hostname]" /> <add initializationPage="/Home/About" hostName="[app hostname]" /> </applicationInitialization> </system.webServer> Reference: <https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots#troubleshoot-swaps> |
| Scenario | You develop and deploy an Azure App Service API app to a Windows-hosted deployment slot named Development. You create additional deployment slots named Testing and Production. You enable auto swap on the Production deployment slot. You need to ensure that scripts run and resources are available before a swap operation occurs. Solution: Enable auto swap for the Testing slot. Deploy the app to the Testing slot. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | Instead update the web.config file to include the applicationInitialization configuration element. Specify custom initialization actions to run the scripts. Note: Some apps might require custom warm-up actions before the swap. The applicationInitialization configuration element in web.config lets you specify custom initialization actions. The swap operation waits for this custom warm-up to finish before swapping with the target slot. Here's a sample web.config fragment. <system.webServer> <applicationInitialization> <add initializationPage="/" hostName="[app hostname]" /> <add initializationPage="/Home/About" hostName="[app hostname]" /> </applicationInitialization> </system.webServer> Reference: <https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots#troubleshoot-swaps> |
| Scenario | You create additional deployment slots named Testing and Production. You enable auto swap on the Production deployment slot. You need to ensure that scripts run and resources are available before a swap operation occurs. Solution: Disable auto swap. Update the app with a method named statuscheck to run the scripts. Re-enable auto swap and deploy the app to the Production slot. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | element. Specify custom initialization actions to run the scripts. Note: Some apps might require custom warm-up actions before the swap. The applicationInitialization configuration element in web.config lets you specify custom initialization actions. The swap operation waits for this custom warm-up to finish before swapping with the target slot. Here's a sample web.config fragment. <system.webServer> <applicationInitialization> <add initializationPage="/" hostName="[app hostname]" /> <add initializationPage="/Home/About" hostName="[app hostname]" /> </applicationInitialization> </system.webServer> Reference: https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots#troubleshoot-swaps |
| Scenario | You develop a software as a service (SaaS) offering to manage photographs. Users upload photos to a web service which then stores the photos in Azure Storage Blob storage. The storage account type is General-purpose V2. When photos are uploaded, they must be processed to produce and save a mobile-friendly version of the image. The process to produce a mobile-friendly version of the image must start in less than one minute. You need to design the process that starts the photo processing. Solution: Convert the Azure Storage account to a BlockBlobStorage storage account. Does the solution meet the goal? |
| Answer | No |
| Explanation | Not necessary to convert the account, instead move photo processing to an Azure Function triggered from the blob upload.. Azure Storage events allow applications to react to events. Common Blob storage event scenarios include image or video processing, search indexing, or any file- oriented workflow. Note: Only storage accounts of kind StorageV2 (general purpose v2) and BlobStorage support event integration. Storage (general purpose v1) does not support integration with Event Grid. Reference: <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-event-overview> |
| Scenario | You develop an HTTP triggered Azure Function app to process Azure Storage blob data. The app is triggered using an output binding on the blob. The app continues to time out after four minutes. The app must process the blob data. You need to ensure the app does not time out and processes the blob data. Solution: Use the Durable Function async pattern to process the blob data. Does the solution meet the goal? |
| Answer | No |
| Explanation | Instead pass the HTTP trigger payload into an Azure Service Bus queue to be processed by a queue trigger function and return an immediate HTTP success response. Note: Large, long-running functions can cause unexpected timeout issues. General best practices include: Whenever possible, refactor large functions into smaller function sets that work together and return responses fast. For example, a webhook or HTTP trigger function might require an acknowledgment response within a certain time limit; it's common for webhooks to require an immediate response. You can pass the HTTP trigger payload into a queue to be processed by a queue trigger function. This approach lets you defer the actual work and return an immediate response. Reference: <https://docs.microsoft.com/en-us/azure/azure-functions/functions-best-practices> |
| Scenario | You develop an HTTP triggered Azure Function app to process Azure Storage blob data. The app is triggered using an output binding on the blob. The app continues to time out after four minutes. The app must process the blob data. You need to ensure the app does not time out and processes the blob data. Solution: Pass the HTTP trigger payload into an Azure Service Bus queue to be processed by a queue trigger function and return an immediate HTTP success response. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | Large, long-running functions can cause unexpected timeout issues. General best practices include: Whenever possible, refactor large functions into smaller function sets that work together and return responses fast. For example, a webhook or HTTP trigger function might require an acknowledgment response within a certain time limit; it's common for webhooks to require an immediate response. You can pass the HTTP trigger payload into a queue to be processed by a queue trigger function. This approach lets you defer the actual work and return an immediate response. Reference: <https://docs.microsoft.com/en-us/azure/azure-functions/functions-best-practices> |
| Scenario | You develop an HTTP triggered Azure Function app to process Azure Storage blob data. The app is triggered using an output binding on the blob. The app continues to time out after four minutes. The app must process the blob data. You need to ensure the app does not time out and processes the blob data. Solution: Configure the app to use an App Service hosting plan and enable the Always On setting. Does the solution meet the goal? |
| Answer | No |
| Explanation | * Instead pass the HTTP trigger payload into an Azure Service Bus queue to be processed by a queue trigger function and return an immediate HTTP success response. Note: Large, long-running functions can cause unexpected timeout issues. General best practices include: Whenever possible, refactor large functions into smaller function sets that work together and return responses fast. For example, a webhook or HTTP trigger function might require an acknowledgment response within a certain time limit; it's common for webhooks to require an immediate response. You can pass the HTTP trigger payload into a queue to be processed by a queue trigger function. This approach lets you defer the actual work and return an immediate response. Reference: <https://docs.microsoft.com/en-us/azure/azure-functions/functions-best-practices> |
| Scenario | You develop a software as a service (SaaS) offering to manage photographs. Users upload photos to a web service which then stores the photos in Azure Storage Blob storage. The storage account type is General-purpose V2. When photos are uploaded, they must be processed to produce and save a mobile-friendly version of the image. The process to produce a mobile-friendly version of the image must start in less than one minute. You need to design the process that starts the photo processing. Solution: Move photo processing to an Azure Function triggered from the blob upload. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | Azure Storage events allow applications to react to events. Common Blob storage event scenarios include image or video processing, search indexing, or any file- oriented workflow. Events are pushed using Azure Event Grid to subscribers such as Azure Functions, Azure Logic Apps, or even to your own http listener. Note: Only storage accounts of kind StorageV2 (general purpose v2) and BlobStorage support event integration. Storage (general purpose v1) does not support integration with Event Grid. Reference: <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-event-overview> |
| Scenario | You develop a software as a service (SaaS) offering to manage photographs. Users upload photos to a web service which then stores the photos in Azure Storage Blob storage. The storage account type is General-purpose V2. When photos are uploaded, they must be processed to produce and save a mobile-friendly version of the image. The process to produce a mobile-friendly version of the image must start in less than one minute. You need to design the process that starts the photo processing. Solution: Move photo processing to an Azure Function triggered from the blob upload. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | Azure Storage events allow applications to react to events. Common Blob storage event scenarios include image or video processing, search indexing, or any file- oriented workflow. Events are pushed using Azure Event Grid to subscribers such as Azure Functions, Azure Logic Apps, or even to your own http listener. Note: Only storage accounts of kind StorageV2 (general purpose v2) and BlobStorage support event integration. Storage (general purpose v1) does not support integration with Event Grid. Reference: https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-event-overview |
| Scenario | You develop Azure solutions. You must grant a virtual machine (VM) access to specific resource groups in Azure Resource Manager. You need to obtain an Azure Resource Manager access token. Solution: Use an X.509 certificate to authenticate the VM with Azure Resource Manager. Does the solution meet the goal? |
| Answer | No |
| Explanation | Instead run the Invoke-RestMethod cmdlet to make a request to the local managed identity for Azure resources endpoint. Reference: <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-arm> |
| Scenario | You develop Azure solutions. You must grant a virtual machine (VM) access to specific resource groups in Azure Resource Manager. You need to obtain an Azure Resource Manager access token. Solution: Use the Reader role-based access control (RBAC) role to authenticate the VM with Azure Resource Manager. Does the solution meet the goal? |
| Answer | No |
| Explanation | Instead run the Invoke-RestMethod cmdlet to make a request to the local managed identity for Azure resources endpoint. Reference: https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-arm |
| Scenario | You develop Azure solutions. You must grant a virtual machine (VM) access to specific resource groups in Azure Resource Manager. You need to obtain an Azure Resource Manager access token. Solution: Run the Invoke-RestMethod cmdlet to make a request to the local managed identity for Azure resources endpoint. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | Get an access token using the VM's system-assigned managed identity and use it to call Azure Resource Manager You will need to use PowerShell in this portion. 1. In the portal, navigate to Virtual Machines and go to your Windows virtual machine and in the Overview, click Connect. 2. Enter in your Username and Password for which you added when you created the Windows VM. 3. Now that you have created a Remote Desktop Connection with the deefffdfgtrtyg machine, open PowerShell in the remote session. 4. Using the Invoke-WebRequest cmdlet, make a request to the local managed identity for Azure resources endpoint to get an access token for Azure Resource Manager. Example: $response = Invoke-WebRequest -Uri 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https:// management.azure.com/' -Method GET -Headers @{Metadata="true"} Reference: <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-arm> |
| Scenario | You are developing and deploying several ASP.NET web applications to Azure App Service. You plan to save session state information and HTML output. You must use a storage mechanism with the following requirements: ✑ Share session state across all ASP.NET web applications. ✑ Support controlled, concurrent access to the same session state data for multiple readers and a single writer. ✑ Save full HTTP responses for concurrent requests. You need to store the information. Proposed Solution: Enable Application Request Routing (ARR). Does the solution meet the goal? |
| Answer | No |
| Explanation | Instead deploy and configure Azure Cache for Redis. Update the web applications. Reference: <https://docs.microsoft.com/en-us/azure/architecture/best-practices/caching#managing-concurrency-in-a-cache> |
| Scenario | You are developing and deploying several ASP.NET web applications to Azure App Service. You plan to save session state information and HTML output. You must use a storage mechanism with the following requirements: ✑ Share session state across all ASP.NET web applications. ✑ Support controlled, concurrent access to the same session state data for multiple readers and a single writer. ✑ Save full HTTP responses for concurrent requests. You need to store the information. Proposed Solution: Deploy and configure an Azure Database for PostgreSQL. Update the web applications. Does the solution meet the goal? |
| Answer | No |
| Explanation | Instead deploy and configure Azure Cache for Redis. Update the web applications. Reference: <https://docs.microsoft.com/en-us/azure/architecture/best-practices/caching#managing-concurrency-in-a-cache> |
| Scenario | You are developing and deploying several ASP.NET web applications to Azure App Service. You plan to save session state information and HTML output. You must use a storage mechanism with the following requirements: Share session state across all ASP.NET web applications.  ✑ Support controlled, concurrent access to the same session state data for multiple readers and a single writer. ✑ Save full HTTP responses for concurrent requests. You need to store the information. Proposed Solution: Deploy and configure Azure Cache for Redis. Update the web applications. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | The session state provider for Azure Cache for Redis enables you to share session information between different instances of an ASP.NET web application. The same connection can be used by multiple concurrent threads. Redis supports both read and write operations. The output cache provider for Azure Cache for Redis enables you to save the HTTP responses generated by an ASP.NET web application. Note: Using the Azure portal, you can also configure the eviction policy of the cache, and control access to the cache by adding users to the roles provided. These roles, which define the operations that members can perform, include Owner, Contributor, and Reader. For example, members of the Owner role have complete control over the cache (including security) and its contents, members of the Contributor role can read and write information in the cache, and members of the Reader role can only retrieve data from the cache. Reference: <https://docs.microsoft.com/en-us/azure/architecture/best-practices/caching> |
| Scenario | You are developing an Azure Service application that processes queue data when it receives a message from a mobile application. Messages may not be sent to the service consistently. You have the following requirements: ✑ Queue size must not grow larger than 80 gigabytes (GB). ✑ Use first-in-first-out (FIFO) ordering of messages. ✑ Minimize Azure costs. You need to implement the messaging solution. Solution: Use the .Net API to add a message to an Azure Storage Queue from the mobile application. Create an Azure VM that is triggered from Azure Storage Queue events. Does the solution meet the goal? |
| Answer | No |
| Explanation | Don't use a VM, instead create an Azure Function App that uses an Azure Service Bus Queue trigger. Reference: <https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-storage-queue-triggered-function> |
| Scenario | You are developing an Azure Service application that processes queue data when it receives a message from a mobile application. Messages may not be sent to the service consistently. You have the following requirements: ✑ Queue size must not grow larger than 80 gigabytes (GB). ✑ Use first-in-first-out (FIFO) ordering of messages. ✑ Minimize Azure costs. You need to implement the messaging solution. Solution: Use the .Net API to add a message to an Azure Service Bus Queue from the mobile application. Create an Azure Windows VM that is triggered from Azure Service Bus Queue. Does the solution meet the goal? |
| Answer | No |
| Explanation | Don't use a VM, instead create an Azure Function App that uses an Azure Service Bus Queue trigger. Reference: <https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-storage-queue-triggered-function> |
| Scenario | You are developing an Azure Service application that processes queue data when it receives a message from a mobile application. Messages may not be sent to the service consistently. You have the following requirements: ✑ Queue size must not grow larger than 80 gigabytes (GB). ✑ Use first-in-first-out (FIFO) ordering of messages. ✑ Minimize Azure costs. You need to implement the messaging solution. Solution: Use the .Net API to add a message to an Azure Service Bus Queue from the mobile application. Create an Azure Function App that uses an Azure Service Bus Queue trigger. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | You can create a function that is triggered when messages are submitted to an Azure Storage queue. Reference: <https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-storage-queue-triggered-function> |
| Scenario | You are developing a website that will run as an Azure Web App. Users will authenticate by using their Azure Active Directory (Azure AD) credentials. You plan to assign users one of the following permission levels for the website: admin, normal, and reader. A user's Azure AD group membership must be used to determine the permission level. You need to configure authorization. Solution: Configure the Azure Web App for the website to allow only authenticated requests and require Azure AD log on. Does the solution meet the goal |
| Answer | No |
| Explanation | Instead in the Azure AD application's manifest, set value of the groupMembershipClaims option to All. Reference: <https://blogs.msdn.microsoft.com/waws/2017/03/13/azure-app-service-authentication-aad-groups/> |
| Scenario | You are developing a website that will run as an Azure Web App. Users will authenticate by using their Azure Active Directory (Azure AD) credentials. You plan to assign users one of the following permission levels for the website: admin, normal, and reader. A user's Azure AD group membership must be used to determine the permission level. You need to configure authorization. Solution: ✑ Create a new Azure AD application. In the application's manifest, set value of the groupMembershipClaims option to All. ✑ In the website, use the value of the groups claim from the JWT for the user to determine permissions. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | To configure Manifest to include Group Claims in Auth Token 1. Go to Azure Active Directory to configure the Manifest. Click on Azure Active Directory, and go to App registrations to find your application: 2. Click on your application (or search for it if you have a lot of apps) and edit the Manifest by clicking on it. 3. Locate the "groupMembershipClaims" setting. Set its value to either "SecurityGroup" or "All". To help you decide which: ✑ "SecurityGroup" - groups claim will contain the identifiers of all security groups of which the user is a member. ✑ "All" - groups claim will contain the identifiers of all security groups and all distribution lists of which the user is a member Now your application will include group claims in your manifest and you can use this fact in your code. Reference: <https://blogs.msdn.microsoft.com/waws/2017/03/13/azure-app-service-authentication-aad-groups/> |
| Scenario | You are developing a website that will run as an Azure Web App. Users will authenticate by using their Azure Active Directory (Azure AD) credentials. You plan to assign users one of the following permission levels for the website: admin, normal, and reader. A user's Azure AD group membership must be used to determine the permission level. You need to configure authorization. Solution: ✑ Create a new Azure AD application. In the application's manifest, define application roles that match the required permission levels for the application. ✑ Assign the appropriate Azure AD group to each role. In the website, use the value of the roles claim from the JWT for the user to determine permissions. Does the solution meet the goal? |
| Answer | No |
| Explanation | * To configure Manifest to include Group Claims in Auth Token 1. Go to Azure Active Directory to configure the Manifest. Click on Azure Active Directory, and go to App registrations to find your application: 2. Click on your application (or search for it if you have a lot of apps) and edit the Manifest by clicking on it. 3. Locate the "groupMembershipClaims" setting. Set its value to either "SecurityGroup" or "All". To help you decide which: ✑ "SecurityGroup" - groups claim will contain the identifiers of all security groups of which the user is a member. ✑ "All" - groups claim will contain the identifiers of all security groups and all distribution lists of which the user is a member Now your application will include group claims in your manifest and you can use this fact in your code. Reference: https://blogs.msdn.microsoft.com/waws/2017/03/13/azure-app-service-authentication-aad-groups/ Monitor, troubleshoot, and optimize Azure solutions |
| Scenario | You are developing a medical records document management website. The website is used to store scanned copies of patient intake forms. If the stored intake forms are downloaded from storage by a third party, the contents of the forms must not be compromised. You need to store the intake forms according to the requirements. Solution: Store the intake forms as Azure Key Vault secrets. Does the solution meet the goal? |
| Answer | No |
| Explanation | Instead use an Azure Key vault and public key encryption. Store the encrypted from in Azure Storage Blob storage. Monitor, troubleshoot, and optimize Azure solutions |
| Scenario | You are developing an Azure solution to collect point-of-sale (POS) device data from 2,000 stores located throughout the world. A single device can produce 2 megabytes (MB) of data every 24 hours. Each store location has one to five devices that send data. You must store the device in Azure Blob storage. Device data must be correlated based on a device identifier. Additional stores are expected to open in the future. You need to implement a solution to receive the device data. Solution: Provision an Azure Event Hub. Configure the machine identifier as the partition key and enable capture. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | References: <https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-programming-guide> |
| Scenario | You are developing an Azure solution to collect point-of-sale (POS) device data from 2,000 stores located throughout the world. A single device can produce 2 megabytes (MB) of data every 24 hours. Each store location has one to five devices that send data. You must store the device in Azure Blob storage. Device data must be correlated based on a device identifier. Additional stores are expected to open in the future. You need to implement a solution to receive the device data. Solution: Provision an Azure Event Grid. Configure event filtering to evaluate the device identifier. Does the solution meet the goal? |
| Answer | No |
| Explanation | References: <https://docs.microsoft.com/en-us/azure/event-grid/event-filtering> |
| Scenario | You are developing an Azure solution to collect point-of-sale (POS) device data from 2,000 stores located throughout the world. A single device can produce 2 megabytes (MB) of data every 24 hours. Each store location has one to five devices that send data. You must store the device in Azure Blob storage. Device data must be correlated based on a device identifier. Additional stores are expected to open in the future. You need to implement a solution to receive the device data. Solution: Provision an Azure Notification Hub. Register all devices with the hub. Does the solution meet the goal? |
| Answer | No |
| Explanation | Instead provision an Azure Event Hub. Configure the machine identifier as the partition key and enable capture. References: <https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-programming-guide> |
| Scenario | Margie's Travel is an international travel and bookings management service. The company is expanding into restaurant bookings. You are tasked with implementing Azure Search for the restaurants listed in their solution. You create the index in Azure Search. You need to import the restaurant data into the Azure Search service by using the Azure Search .NET SDK. Solution: 1. Create a SearchServiceClient object to connect to the search index. 2. Create a DataContainer that contains the documents which must be added. 3. Create a DataSource instance and set its Container property to the DataContainer. 4. Call the Documents.Suggest method of the SearchIndexClient and pass the DataSource. Does the solution meet the goal? |
| Answer | No |
| Explanation | Use the following method: 1. - Create a SearchIndexClient object to connect to the search index 2. - Create an IndexBatch that contains the documents which must be added. 3. - Call the Documents.Index method of the SearchIndexClient and pass the IndexBatch. References: <https://docs.microsoft.com/en-us/azure/search/search-howto-dotnet-sdkds> |
| Scenario | Margie's Travel is an international travel and bookings management service. The company is expanding into restaurant bookings. You are tasked with implementing Azure Search for the restaurants listed in their solution. You create the index in Azure Search. You need to import the restaurant data into the Azure Search service by using the Azure Search .NET SDK. Solution: 1. Create a SearchIndexClient object to connect to the search index 2. Create an IndexBatch that contains the documents which must be added. 3. Call the Documents.Index method of the SearchIndexClient and pass the IndexBatch. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | 1. The index needs to be populated. To do this, we will need a SearchIndexClient. There are two ways to obtain one: by constructing it, or by calling Indexes.GetClient on the SearchServiceClient. Here we will use the first method. 2. Create the indexBatch with the documents Something like: var hotels = new Hotel[]; { new Hotel() { HotelId = "3", BaseRate = 129.99, Description = "Close to town hall and the river" } }; "¦ var batch = IndexBatch.Upload(hotels); 3. The next step is to populate the newly-created index Example: var batch = IndexBatch.Upload(hotels); try { indexClient.Documents.Index(batch); } References: <https://docs.microsoft.com/en-us/azure/search/search-howto-dotnet-sdk> |
| Scenario | You need to ensure that the SecurityPin security requirements are met. 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 | Enable Always Encrypted is correct, but only the WebAppIdentity service principal should be given access to the certificate. 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 |
| Scenario | You need to ensure that the SecurityPin security requirements are met. Solution: Using the Azure Portal, add Data Masking to the SecurityPin column, and exclude the dbo user. Add a SQL security policy with a filter predicate based on the user identity. Does the solution meet the goal? |
| Answer | No |
| Explanation | Instead of DataMasing, enable Always Encrypted for the SecurityPin column. 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 |
| Scenario | 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. |
| Scenario | 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. |
| Scenario | You are developing a solution that will be deployed to an Azure Kubernetes Service (AKS) cluster. The solution will include a custom VNet, Azure Container Registry images, and an Azure Storage account. The solution must allow dynamic creation and management of all Azure resources within the AKS cluster. You need to configure an AKS cluster for use with the Azure APIs. Solution: Enable the Azure Policy Add-on for Kubernetes to connect the Azure Policy service to the GateKeeper admission controller for the AKS cluster. Apply a built-in policy to the cluster. Does the solution meet the goal? |
| Answer | No |
| Explanation | Instead create an AKS cluster that supports network policy. Create and apply a network to allow traffic only from within a defined namespace References: <https://docs.microsoft.com/en-us/azure/aks/use-network-policies> |
| Scenario | You are developing a solution that will be deployed to an Azure Kubernetes Service (AKS) cluster. The solution will include a custom VNet, Azure Container Registry images, and an Azure Storage account. The solution must allow dynamic creation and management of all Azure resources within the AKS cluster. You need to configure an AKS cluster for use with the Azure APIs. Solution: Enable the Azure Policy Add-on for Kubernetes to connect the Azure Policy service to the GateKeeper admission controller for the AKS cluster. Apply a built-in policy to the cluster. Does the solution meet the goal? |
| Answer |  |
| Explanation | Instead create an AKS cluster that supports network policy. Create and apply a network to allow traffic only from within a defined namespace References: <https://docs.microsoft.com/en-us/azure/aks/use-network-policies> |
| Scenario | You are developing a solution that will be deployed to an Azure Kubernetes Service (AKS) cluster. The solution will include a custom VNet, Azure Container Registry images, and an Azure Storage account. The solution must allow dynamic creation and management of all Azure resources within the AKS cluster. You need to configure an AKS cluster for use with the Azure APIs. Solution: Create an AKS cluster that supports network policy. Create and apply a network to allow traffic only from within a defined namespace. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | When you run modern, microservices-based applications in Kubernetes, you often want to control which components can communicate with each other. The principle of least privilege should be applied to how traffic can flow between pods in an Azure Kubernetes Service (AKS) cluster. Let's say you likely want to block traffic directly to back-end applications. The Network Policy feature in Kubernetes lets you define rules for ingress and egress traffic between pods in a cluster. References: https://docs.microsoft.com/en-us/azure/aks/use-network-policies Develop Azure Platform as a Service Compute Solutions |
| Scenario | You connect to Azure by using a workstation that has a slow internet connection. You have two Azure file shares. You plan to transfer a series of large files from one container to another container. The workstation does not have sufficient disk space to store the files. You define the following variables in Azure PowerShell:  You need to simultaneously transfer the large files as efficiently as possible. Solution: Write a C# application that implements the Azure Storage API method CloudFile.StartCopy to transfer files to the destination container. Does the solution meet the goal? |
| Answer | No |
| Explanation | Use AzCopy - References: <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy> |
| Scenario | You connect to Azure by using a workstation that has a slow internet connection. You have two Azure file shares. You plan to transfer a series of large files from one container to another container. The workstation does not have sufficient disk space to store the files. You define the following variables in Azure PowerShell:  You need to simultaneously transfer the large files as efficiently as possible. Solution: Run the following Azure PowerShell command: AzCopy /Source:$sourceServer /Dest:$DestServer /SourceKey:$sourcekey /DestKey:$destKey /S Does the solution meet the goal? |
| Answer | Yes |
| Explanation | https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy |
| Scenario | You connect to Azure by using a workstation that has a slow internet connection. You have two Azure file shares. You plan to transfer a series of large files from one container to another container. The workstation does not have sufficient disk space to store the files. You define the following variables in Azure PowerShell:  You need to simultaneously transfer the large files as efficiently as possible. Solution: Run the following Azure PowerShell command: AzCopy /Source:$sourceServer /Dest:C:\Files /SourceKey:$sourceKey /S Does the solution meet the goal? |
| Answer | No |
| Explanation | The /Dest parameter should be :$DestServer, not C:\Files. References: https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy |
| Scenario | ou have the following resource groups:  Developers must connect to DevServer only through DevWorkstation. To maintain security, DevServer must not accept connections from the internet. You need to create a private connection between the DevWorkstation and DevServer. Solution: Configure an IP address on each subnet within the same address space. Does the solution meet the goal? |
| Answer | No |
| Explanation | Use Global Virtual Network peering. Azure Global Virtual Network peering allows you to peer virtual networks in different Azure regions to build a global private network in Azure. References: <https://azure.microsoft.com/en-us/updates/global-vnet-peering/> |
| Scenario | You have the following resource groups:  Developers must connect to DevServer only through DevWorkstation. To maintain security, DevServer must not accept connections from the internet. You need to create a private connection between the DevWorkstation and DevServer. Solution: Configure Global Virtual Network peering between the two Virtual Networks and configure network security groups to allow connectivity between the DevServer and the DevWorkstation using their private IP addresses. Does the solution meet the goal? |
| Answer | Yes |
| Explanation | Azure Global Virtual Network peering allows you to peer virtual networks in different Azure regions to build a global private network in Azure. References: <https://azure.microsoft.com/en-us/updates/global-vnet-peering/> |
| Scenario | You have the following resource groups:  Developers must connect to DevServer only through DevWorkstation. To maintain security, DevServer must not accept connections from the internet. You need to create a private connection between the DevWorkstation and DevServer. Solution: Configure a public IP address on DevServer\_WestCentral. Configure the Network Security Group to allow all incoming ports. Does the solution meet the goal? |
| Answer | No |
| Explanation | DevServer must not accept connections from the internet. Instead use Global Virtual Network peering. Azure Global Virtual Network peering allows you to peer virtual networks in different Azure regions to build a global private network in Azure. References: <https://azure.microsoft.com/en-us/updates/global-vnet-peering/> |
| Scenario |  |
| Answer |  |
| Explanation |  |
| Scenario |  |
| Answer |  |
| Explanation |  |
| Scenario |  |
| Answer |  |
| Explanation |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |