

- Expert Verified, Online, Free.

Custom View Settings

Question #10 Topic 4

You develop a gateway solution for a public facing news API. The news API back end is implemented as a RESTful service and uses an OpenAPI specification.

You need to ensure that you can access the news API by using an Azure API Management service instance.

Which Azure PowerShell command should you run?

- A. Import-AzureRmApiManagementApi -Context \$ApiMgmtContext -SpecificationFormat "Swagger" -SpecificationPath \$SwaggerPath -Path \$Path
- B. New-AzureRmApiManagementBackend -Context \$ApiMgmtContext-Url \$Url -Protocol http
- C. New-AzureRmApiManagement -ResourceGroupName \$ResourceGroup -Name \$Name a€"Location \$Location -Organization \$Org AdminEmail \$AdminEmail
- D. New-AzureRmApiManagementBackendProxy -Url \$ApiUrl

Correct Answer: D 🥕

New-AzureRmApiManagementBackendProxy creates a new Backend Proxy Object which can be piped when creating a new Backend entity. Example: Create a Backend Proxy In-Memory Object

PS C:\>\$secpassword = ConvertTo-SecureString "PlainTextPassword" -AsPlainText -Force

PS C:\>\$proxyCreds = New-Object System.Management.Automation.PSCredential ("foo", \$secpassword)

PS C:\>\$credential = New-AzureRmApiManagementBackendProxy -Url "http://12.168.1.1:8080" -ProxyCredential \$proxyCreds

PS C:\>\$apimContext = New-AzureRmApiManagementContext -ResourceGroupName "Api-Default-WestUS" -ServiceName "contoso"

PS C:\>\$backend = New-AzureRmApiManagementBackend -Context \$apimContext -BackendId 123 -Url 'https://contoso.com/awesomeapi' -

Protocol http -Title

"first backend" -SkipCertificateChainValidation \$true -Proxy \$credential -Description "backend with proxy server"

Creates a Backend Proxy Object and sets up Backend

Incorrect Answers:

A: The Import-AzureRmApiManagementApi cmdlet imports an Azure API Management API from a file or a URL in Web Application Description Language (WADL),

Web Services Description Language (WSDL), or Swagger format.

B: New-AzureRmApiManagementBackend creates a new backend entity in Api Management.

C: The New-AzureRmApiManagement cmdlet creates an API Management deployment in Azure API Management.

Reference:

https://docs.microsoft.com/en-us/powershell/module/azurerm.apimanagement/new-azurermapimanagementbackendproxy?view=azurermps-6.13.0

Question #11

You are creating a hazard notification system that has a single signaling server which triggers audio and visual alarms to start and stop.

You implement Azure Service Bus to publish alarms. Each alarm controller uses Azure Service Bus to receive alarm signals as part of a transaction. Alarm events must be recorded for audit purposes. Each transaction record must include information about the alarm type that was activated.

You need to implement a reply trail auditing solution.

Which two actions should you perform? Each correct answer resents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Assign the value of the hazard message SessionID property to the ReplyToSessionId property.
- B. Assign the value of the hazard message Messageld property to the DevileryCount property.
- C. Assign the value of the hazard message SessionID property to the SequenceNumber property.
- D. Assign the value of the hazard message Messageld property to the CorrelationId property.
- E. Assign the value of the hazard message SequenceNumber property to the DeliveryCount property.
- F. Assign the value of the hazard message Messageld property to the SequenceNumber property.

Correct Answer: AD 🥕

D: CorrelationId: Enables an application to specify a context for the message for the purposes of correlation; for example, reflecting the MessageId of a message that is being replied to.

A: ReplyToSessionId: This value augments the ReplyTo information and specifies which SessionId should be set for the reply when sent to the reply entity.

Incorrect Answers:

B, E: DeliveryCount -

Number of deliveries that have been attempted for this message. The count is incremented when a message lock expires, or the message is explicitly abandoned by the receiver. This property is read-only.

C, E: SequenceNumber -

The sequence number is a unique 64-bit integer assigned to a message as it is accepted and stored by the broker and functions as its true identifier. For partitioned entities, the topmost 16 bits reflect the partition identifier. Sequence numbers monotonically increase and are gapless. They roll over to 0 when the 48-

64 bit range is exhausted. This property is read-only.

Reference:

https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-messages-payloads

Topic 4 Question #12

You are developing an Azure function that connects to an Azure SQL Database instance. The function is triggered by an Azure Storage queue.

You receive reports of numerous System.InvalidOperationExceptions with the following message:

`Timeout expired. The timeout period elapsed prior to obtaining a connection from the pool. This may have occurred because all pooled connections were in use and max pool size was reached.`

You need to prevent the exception.

What should you do?

- A. In the host.json file, decrease the value of the batchSize option
- B. Convert the trigger to Azure Event Hub
- C. Convert the Azure Function to the Premium plan
- D. In the function.json file, change the value of the type option to queueScaling

Correct Answer: C

With the Premium plan the max outbound connections per instance is unbounded compared to the 600 active (1200 total) in a Consumption plan.

Note: The number of available connections is limited partly because a function app runs in a sandbox environment. One of the restrictions that the sandbox imposes on your code is a limit on the number of outbound connections, which is currently 600 active (1,200 total) connections per instance. When you reach this limit, the functions runtime writes the following message to the logs: Host thresholds exceeded: Connections. Reference:

https://docs.microsoft.com/en-us/azure/azure-functions/manage-connections https://docs.microsoft.com/en-us/azure/azure-functions/manage-connections https://docs.microsoft.com/en-us/azure/azure-functions/manage-connections https://docs.microsoft.com/en-us/azure-functions/manage-connections https://docs.microsoft.com/en-us/azure-functions/manage-connections-function functions/functions-scale#service-limits

Question #13

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution.

Determine whether the solution meets the stated goals.

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?

A. Yes

B. No

Correct Answer: A 🤌

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

Question #14

HOTSPOT -

You are debugging an application that is running on Azure Kubernetes cluster named cluster1. The cluster uses Azure Monitor for containers to monitor the cluster.

The application has sticky sessions enabled on the ingress controller.

Some customers report a large number of errors in the application over the last 24 hours.

You need to determine on which virtual machines (VMs) the errors are occurring.

How should you complete the Azure Monitor query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



