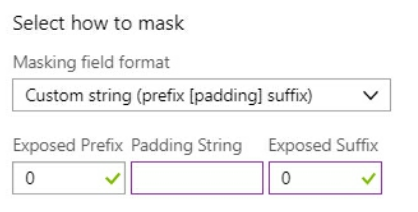
# Misc

Devs want to publish Azure function from VS2019, what to install? **Azure development workload**

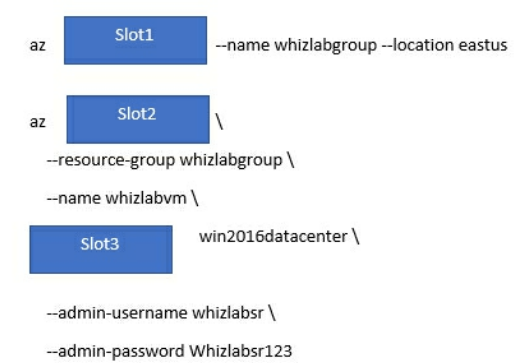
We have external partners who needs access (own credentials, authenticate with their own identity management solution): **Azure B2B**todo: review Azure B2C, B2B, Self-service, Organizational Units

We need data masking for a column in the DB, so it looks like this: XXXX-XX-1234  
  
What should be exposed prefix: 0 (we expose only suffix)  
What should be exposed suffix: 4

CRON expression, we want it to run once every two hours:  
is this ok? 0 0 \*/2 \* \* \*

**Yes: todo cron expressions**

# VM

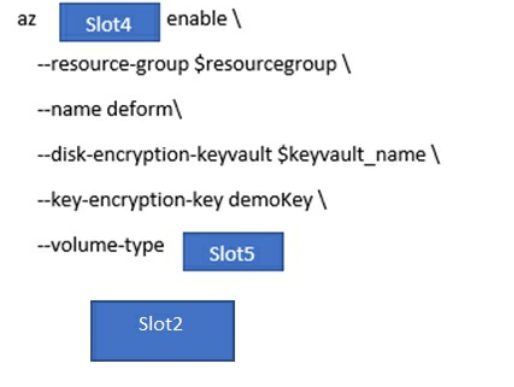


Slot 1: group create  
Slot 2: vm create  
Slot 3: --image

# VM Encryption

We are securing a Linux VM with Disk Encryption





Slot 1: keyvault  
Slot 2: keyvault key  
Slot 3: vm  
Slot 4: vm encryption  
**Slot 5: all**

We want a VM to be encrypted with keys from KeyVault:

1. New-AzVm
2. Get-AzKeyVault
3. Set-AzVmDiskEncryptionExtension

# Search

A team has created an Index.  
We have to upload to the index  
**DO:**

* Create **SearchServiceClient** object to connect to the search index
* Create **DataContainer** which contains the documents which must be added
* Create a **DataSource** instance and set its Container prop to the **DataContainer**
* Set the **DataSource** property of the **ServiceServiceClient** to the created one

**DO NOT:**

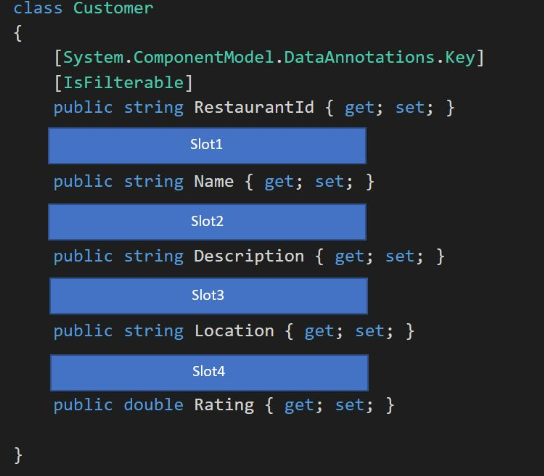
* Create SearchIndexClient, IndexBatch and call Documents.Index

Which object to use to create indexes in Azure Search?

* **SearchServiceClient**
* **SearchCredentials**

We want to use RegEx with search: **use QueryType of Full Lucense search**We want results organized as counts for name-value pairs: **use** **Facets**We want to list products via particular price range: **use Filters**

**Check again these, questions 99**



Search for resturants by name, description, location, cuisine

Narrow results further by location, cuisine, rating, family-friendliness

All words in description must be included in searches

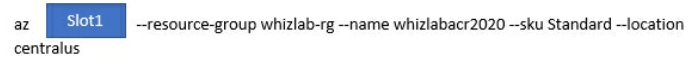
Slot 1: [IsSearchable]  
Slot 2: [IsSearchable, **Required**]  
Slot 3: [IsSearchable, IsFilterable]  
Slot 4: [IsSearchable, IsFilterable]

Todo: check Required attribute

We have a Search Service, where a column was not marked as Searchable, but now it is – would a search work immediately? **No, we have to rebuild the entire index again**

We are creating Search with 2 partitions and 2 replicas with PowerShell:  
New-AzSearchService  
-ResourceGroupName "skillcertlab-rg"  
-Name "skillcertlab-searchapp"  
-Sku "Standard"  
-Location "West US"  
-PartitionCount 2  
-ReplicaCount 2

# Azure Container Registry

Deploying Azure Container RegistrySlot 1: **acr create**

# Kubernetes

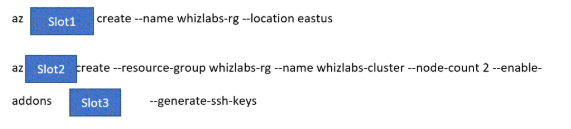
Create Kubernetes cluster:

* az group create
* az aks create
* az aks get-credentials
* kubectl apply

Deploying a new Kubernetes cluster:  
- build new app image by using dockerfile  
- download image to local computer  
- log into the registry and push the image

We have a Web App, which is accessed by another app from Kubernetes  
CHECK QUESTION 101

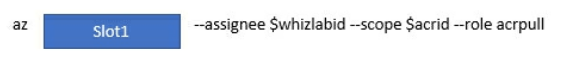
We are deploying AKS cluster:



Slot1: group  
Slot2: aks  
Slot3: monitoring (case study said so: Azure Monitor Container Health must be used to monitor the performance of workloads that are deployed to Kubernetes environments)

We have an app deployed to Kubernetes service, docker images stored in Container Registry  
We need to **deploy an updated version of the app to the cluster**  
- Create updated container image  
- Push the container image to the Container registry  
- Deploy the updated container image

**When creating AKS cluster, this is fine:**az aks create  
--resource-group skillcertlabs-rg  
--name skillcertlabscluster  
--node-count 1  
--enable-addons monitoring  
--generate-ssh-keys

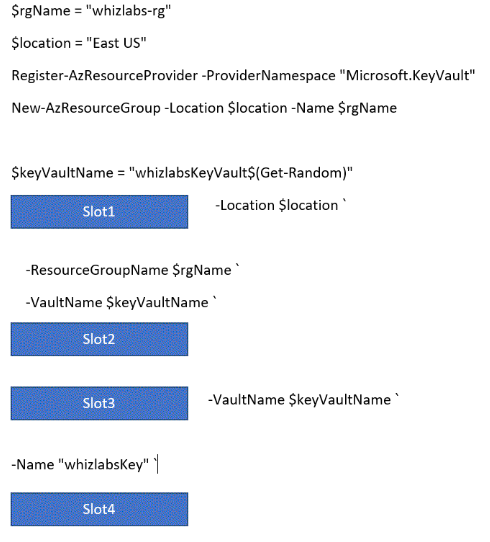
Kubernetes have rights to pull images from ACR:  
  
Slot 1: **role assignment** <https://docs.microsoft.com/en-us/azure/aks/tutorial-kubernetes-prepare-acr>

# Key Vault

We want to create a key in KeyVault via REST API:  
POST https://skillcertlabvault.vault.azure.net/keys/skillcertlabkey/create?api-version=7.0

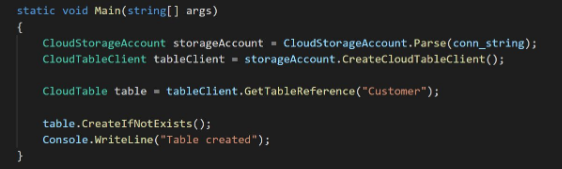
Key Vault REST API to create key (called demokey): https://skillcertlabvault.vault.azure.net/keys/demokey/create?api-version=7.0

Body:  
   
Slot 1: key\_size  
Slot 2: **key\_ops** (these are the allowed operations on the key: <https://docs.microsoft.com/en-us/rest/api/keyvault/createkey/createkey>



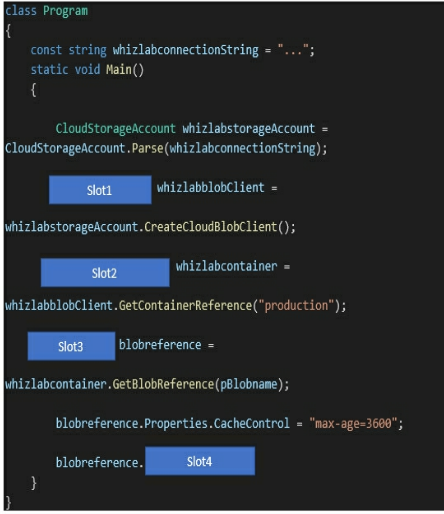
Slot 1: New-AzKeyVault  
Slot 2: -EnabledForDiskEncryption  
Slot 3: Add-AzureKeyVaultKey  
Slot 4: -Destination “Software”

# Azure Storage Account

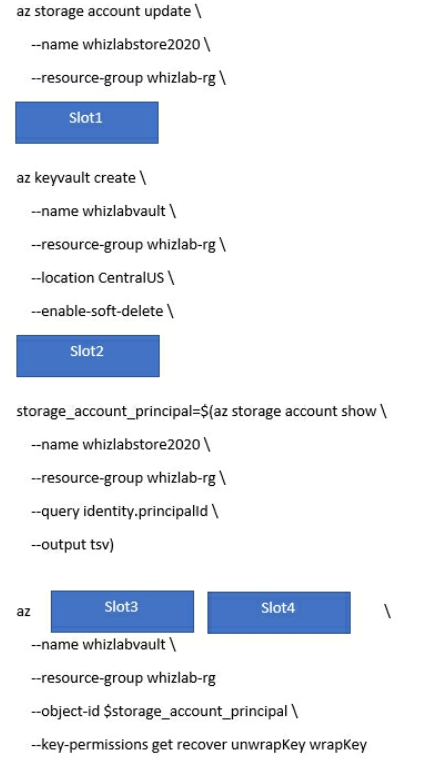


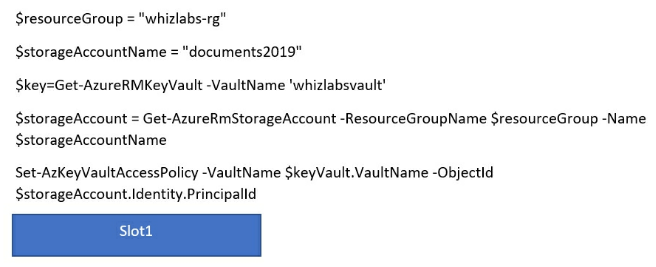
Can this create table Customer? **Yes, if connection string is provided**Can this work with CosmosDB? **Yes**Can this work with Azure Storage? **Yes 🡪 TableAPI is both for Azure Storage and CosmosDB**

We want to store files for 1 year, they won’t get accessed a lot: **use Blob Storage, Archieve tier  
Note, if we want to access these files, then change the tier of the object**

Storage account + CDN, set cache control for Blob in storage  


Slot 1: CloudBlobClient  
Slot 2: CloudBlobContainer  
Slot 3: CloudBlob  
Slot 4: SetProperties

Storage account, ensure data is encrypted at rest with key from key vault:  
  
Slot 1: **--assign identity**  
Slot 2: **--enable-purge-protection**  
Slot 3: keyvault  
Slot 4: set-policy  
<https://docs.microsoft.com/en-us/azure/storage/common/storage-encryption-keys-cli>

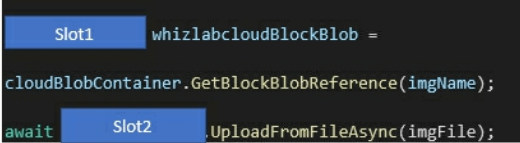
  
(we are ensuring that the right script is in place to ensure that the storage account can use customer managed keys in the key vault)  
**-PermissionsToKeys wrapkey, unwrapkey, get**

[**https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption-customer-managed-keys**](https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption-customer-managed-keys)

want to enbable lease on a blob with REST:

https://skillcertlabstore2020.blob.core.windows.net/demo/skillcertlabcommon.json?**[SLOT1]**Slot 1: **comp=lease**

<https://docs.microsoft.com/en-us/rest/api/storageservices/lease-blob>



Uploading to blob  
Slot 1: **CloudBlockBlob**  
Slot 2: **CloudBlockBlob**

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-quickstart-blobs-dotnet>

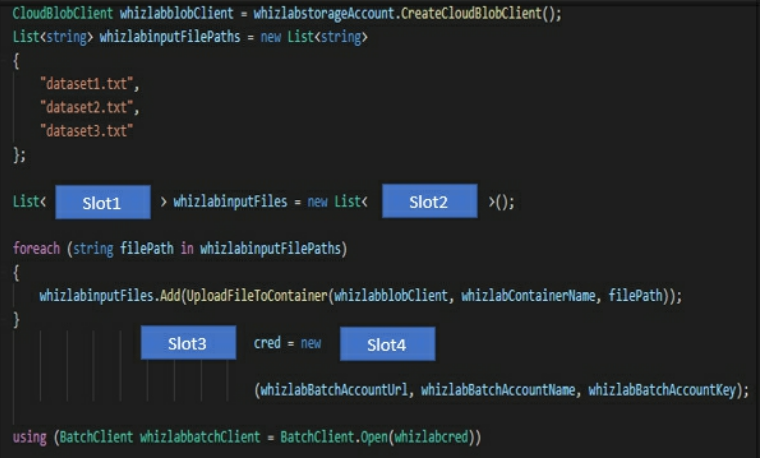
We are using azcopy tool to copy objects from local folder (D:\demo) to storage account  
  
Slot 1: D:\demo (the local folder)  
Slot 2: <https://skillcertlabstore2020.blob.core.windows.net/demo> (full URI of blob container)  
**Slot 3: --recursive=true**

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

# Azure Blob Storage

BLOB storage: concurrent updates shall not happen for same BLOB object: what to implement?  
**Set a Lease for the BLOB**

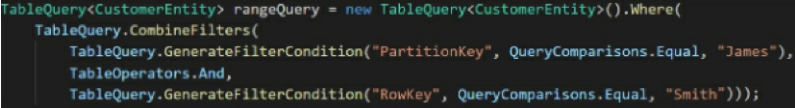
**Todo:** <https://docs.microsoft.com/en-us/rest/api/storageservices/lease-blob>  
also check set blob props, metadata, snapshot

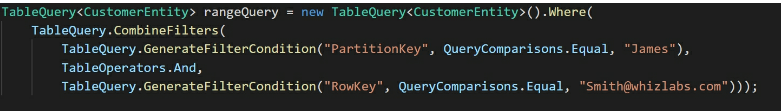
Slot 1: **RESOURCE FILE**  
Slot 2: RESOURCE FILE  
Slot 3: **BatchSharedKeyCredentials**  
Slot 4: BatchSharedKeyCredentials

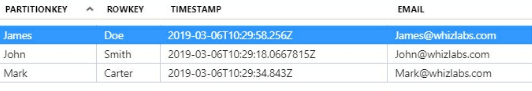
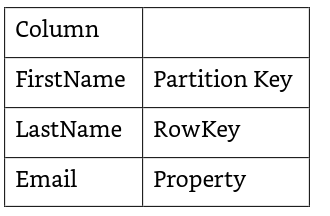
We have a report in BLOB and SQL DB that we want to access (linked in an email that must be valid if the user forwards the mail too)  
**Create a SharedAccessBlobPolicy and set the expiry time to two weeks from today.  
Call GetSharedAccessSignature on the blob and use the resulting link**

(created on the blob, not on the container, because we want to grant the least amount of access)

# Azure Table Storage

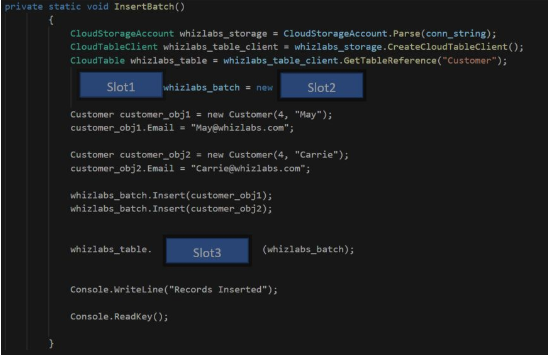
****Is this the same as the REST call /Customer(PartitionKey='James',RowKey='Smith')  
**Yes**

****Does this return all entities where rowkey is [Smith@skillcertlabs.com](mailto:Smith@skillcertlabs.com)  
**No, because AND filter on James**

We have table storage:  


We want FirstName = “James”  
TableQuery query = new TableQuery().Where(TableQuery.GenerateFilterCondition("**PartitionKey**", QueryComparisons.Equal, "James"));

**DO NOT USE FirstName – its not a column, it’s called PartitionKey**



Slot 1: TableBatchOperation  
Slot 2: TableBatchOperation  
Slot 3: ExecuteBatch

Querying from Azure storage (table Customers, partitioned by column firstname)  
Get all „Dave”s:

**TableQuery.GenerateFilterCondition(„PartitionKey”, QueryComparions.Equal, „Dave”)**

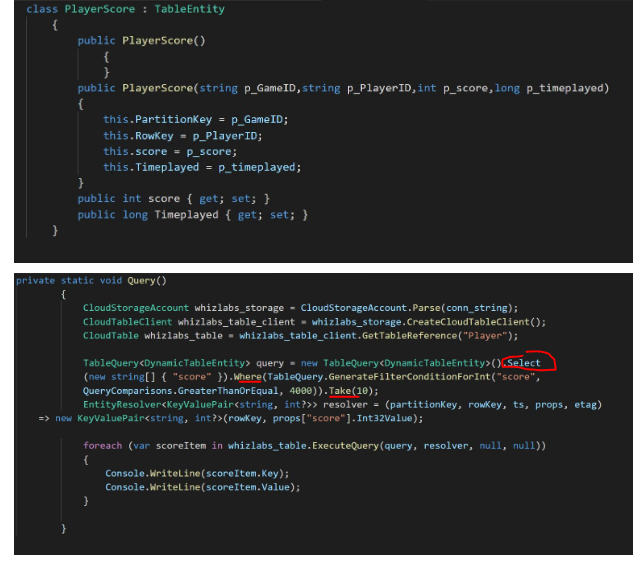
Table Storage:

* What is the parition key: The field with which we want to load balance the data
* What is the row key: Must have value



Slot 3: CloudTable  
Slot 4: TableOperation retrieve = TableOperation.Retrieve(p\_partitionKey, p\_rowKey)

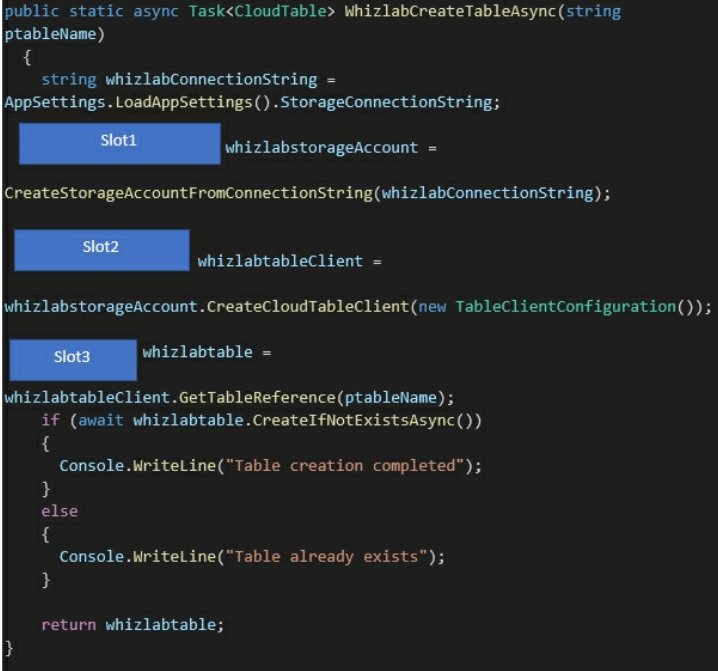
This is valid:



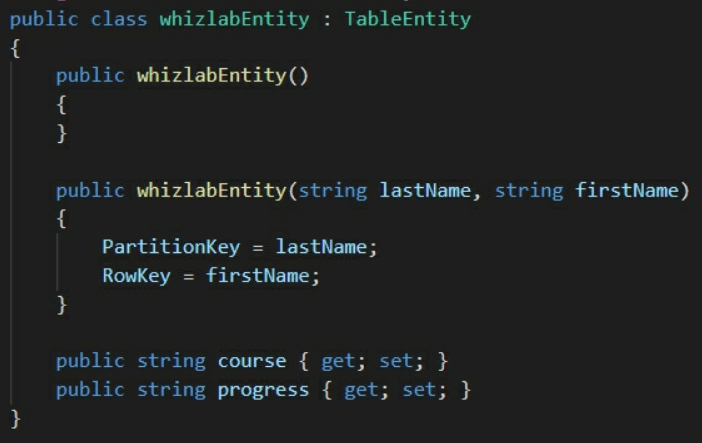
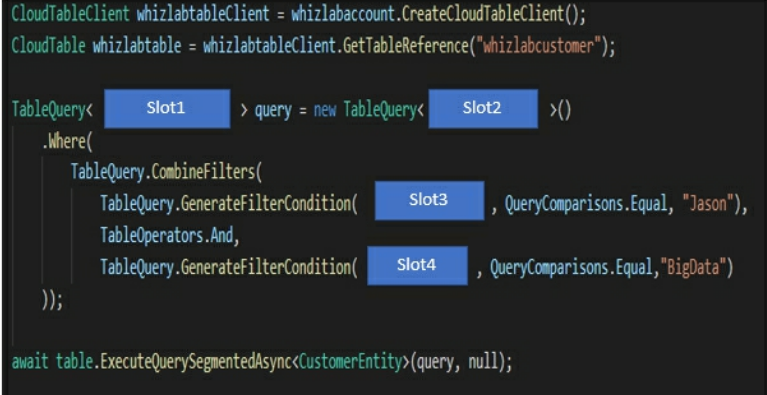
Fetch top 10 rows from table Customer via REST API from Table Storage:  
**https://skillcertlabstore2020.table.core.windows.net/Customers/10**

<https://docs.microsoft.com/en-us/rest/api/storageservices/querying-tables-and-entities>

Some users needs some access to some tables from storage: **DO NOT USE ACCESS KEYS (provides access to EVERYTHING in storage account)  
DO NOT USE ACCESS TOKENS  
USE SHARED ACCESS SIGNATURES (to limit to just Azure Table storage)**

We are interacting with Table storage from .NET  


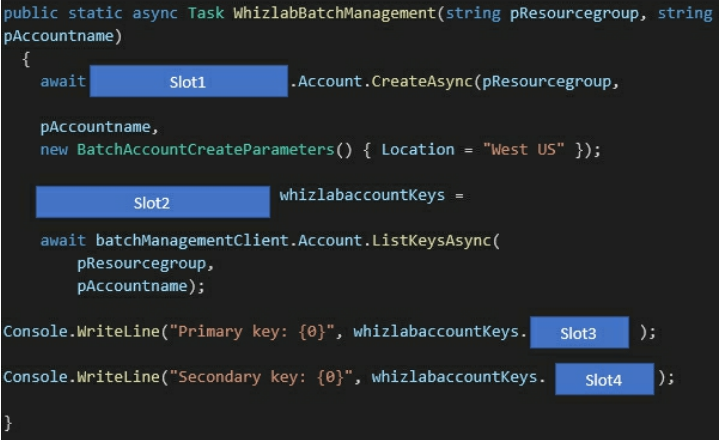
Slot 1: CloudStorageAccount  
Slot 2: CloudTableClient  
Slot 3: CloudTable

We have this: **“Get the customer whose last name is Jason, and course name is BigData”**  
  
  
Slot 1: whizlabEntity  
Slot 2: whizlabEntity  
Slot 3: lastName  
Slot 4: course  
 **?????  
NOTE: Apparently PartitionKey is not used in queries, refer to them as their normal column names  
This is not the case for PrimaryKeys  
??????**

# Batch Service

Azure Batch Service: create compute nodes 🡪 BatchClient.PoolOperations.CreatePool()  
Azure Batch Service: submit a job 🡪 JobOperations.CreateJob() + CloudJob.CommitAsync(Ienumerable, CancellationToken)

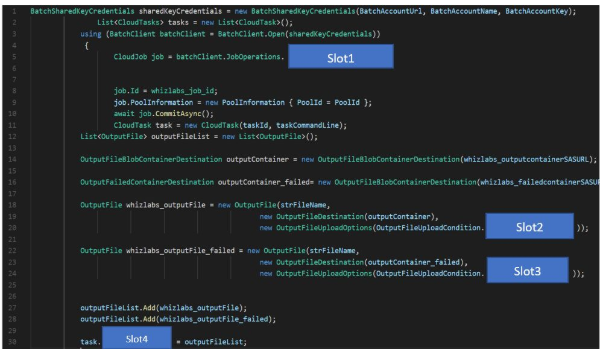
I have a Batch Service’s code, it should put its output to Storage account: **DO NOT get access keys of storage account and submit them to batch job, NOR use CORS (...) 🡪 use SAS (shared access signature)**

We are to interact with Batch Service (create account, retrieve keys)  
  
Slot 1: BatchManagementClient  
Slot 2: BatchAccountListKeyResult  
Slot 3: Primary  
Slot 4: Secondary

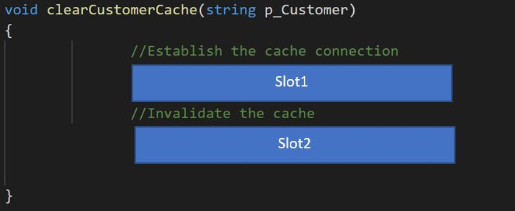
We have an Azure CLI script to work with Batch Service, what’s the good order to run?



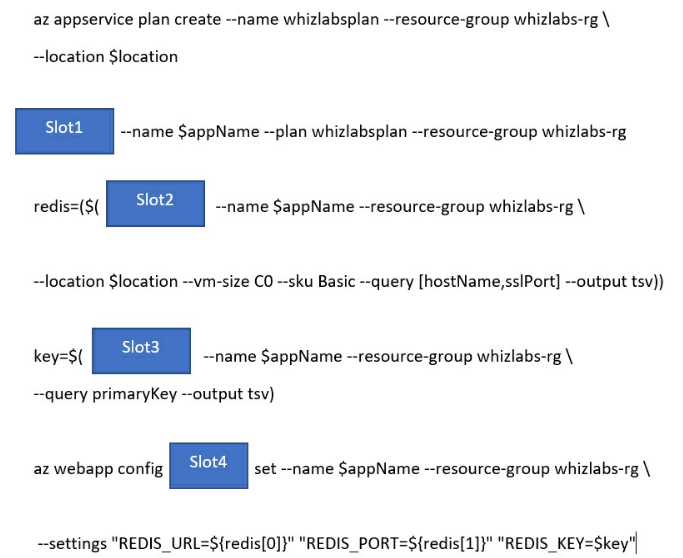
2, 4, 3, 1

  
Slot 1: CreateJob  
Slot 2: TaskSuccess  
Slot 3: TaskFailure  
Slot 4: OutputFiles

# Redis



Redis cache  
Slot 1: IDatabase cache = Connection.GetDatabase();  
Slot 2: cache.KeyDelete(p\_Customer);

WebApp with Redis  


Slot 1: az webapp create  
Slot 2: az redis create  
Slot 3: az redis list-keys  
Slot 4: appsettings

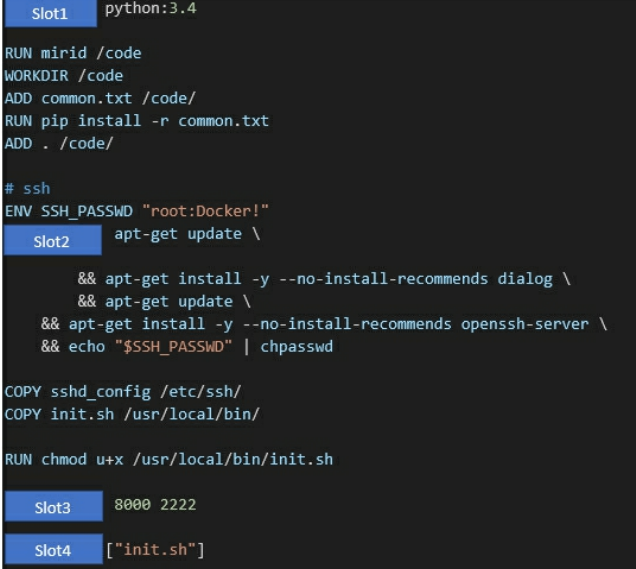
What to store in Redis cache: **Session state** (not HttpContext.Items, ViewState or TempData)

* Cache aside: load data from DB only when needed
* Content caching: static content
* User session caching: shopping carts, etc (before they used to use cookies, but they can grow, have to be validated, etc 🡪 use cookie as the key to the cache/db)
* Job and messauge queuing
* Distributed transaction

# Dockerfile

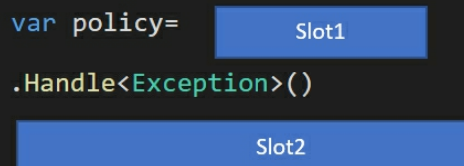
Create Dockerfile, with: application skillcertlabs.dll runs at startup, run a powershell script (both files are in the same directory as Dockerfile)

FROM microsoft/dotnet:2.-aspnetcore-runtime  
ENTRYPOINT[„dotnet”, „skillcertlabs.dll”]  
RUN powershell „skillcertlabsscript.ps1”

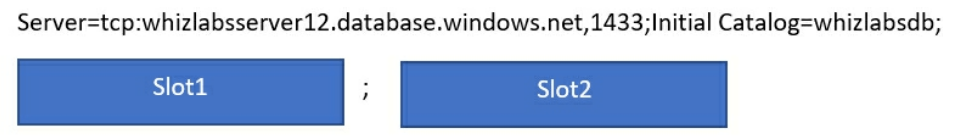
  
Slot 1: FROM  
Slot 2: RUN  
Slot 3: EXPONSE  
Slot 4: **ENTRYPOINT**

# SQL Database

We are modifying Database.cs, to ensure retries are in place for any DB failure

  
Slot 1: new Policy  
Slot 2: WaitAndRetryAsync

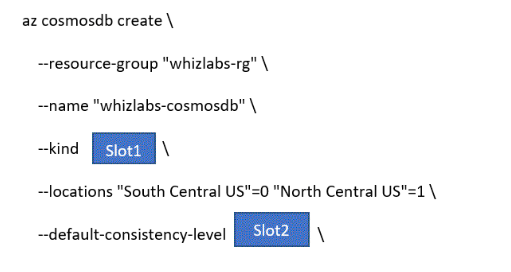
**SQL DB, we want encrypted connection:**  
Set Encrypt=True  
Set **TrustServerCertificate**=False

  
Slot 1: Integrated Security=SSPI (uses Windows authentication)  
Slot 2: Encrypt=True (encrypt data in transit)

We have a SQL DB, with a column „SSN” to which external company should have no access: **use Enable AlwaysOn encryption**

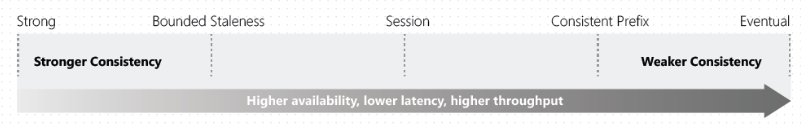
* Incorrect answers include:
  + set column encryption as disabled,
  + Assign users to public fixed database role
  + Store column encryption keys in system catalogue view of the DB (nope, should be always in KeyVault)

# CosmosDB

  
Requirement: we are using SQL queriesSlot1: **GlobalDocumentDB** (todo: review JSON, MongoDB, SQL options for **kind**)  
Slot2: whichever most suited from question

CosmosDB for hospital patients, requirements:

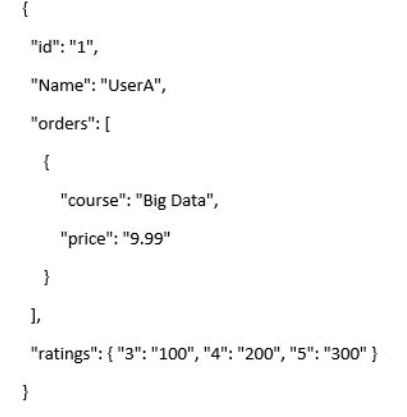
1. Status of patient must be the most recent (even if multiple users in different locations update the same patient’s records) 🡪 STRONG CONSISTENCY
2. Health of patient is recorded by one module, here it needs to be unsured that the data must be either the current version, or the previous version 🡪 BOUNDED STALENESS
3. If patient discharged, all charges to be processed, final bill processed 🡪 EVENTUAL CONSISTENCY



1. **Strong:** Reads return the most recent version (pricey)
2. **Bounded staleness:** Reads consistent with a **preconfigured lag**
   1. Lag can consist of a number of the most recent (K) versions or time interval (T)
3. **Session:** client session scope, best balance between strong consistency and performance by eventual consistency (best where writes occur in the context of a single user)
4. **Consistent Prefix:** Always read in the same order as I write (no guarantee that I can read all the data)
   1. If I write A, B, C then I can read: A or A,B or A,B,C (but never A,C or B,A,C)
5. **Eventual Consistency:** no guarantee for order

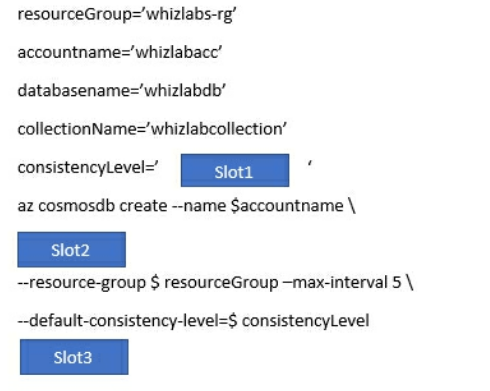
We are developing multiple apps, all of which use separate CosmosDB accounts

App A: not critical app, no orders of reads is required 🡪 **Eventual Consistency**  
App B: must never see out of order writes 🡪 **Consistent Prefix**  
App C: users must see the latest committed write 🡪 **Strong**  
App D: data can be stale by at most 2 versions 🡪 **Bounded Staleness**

We have a web app, users upload images to Blob storage  
This is sent to Azure Function, then into Cosmos DB:  
  
We want to get all items where order price is 9.99

  
Slot 1: customers.orders  
Slot 2: c.price

CosmosDb, we want 99.99% availability, accept writes even if network outage, or failures are happening  
Process data in the same sequence as writes are made  
Allow out of order data with max 5s tolarence  
Use SQL API



Slot1: BoundedStaleness  
Slot 2: --enable-automatic-failover true  
Slot 3: --locations ‘southcentalus=0 eastus=1’ (we are defining two, because of failover rate)

We are updating CosmosDB account, to ensure **failover rate is in place**

az cosmosdb update \  
--name "skillcertlabscosmosdb" \  
--resource-group "skillcertlabs-rg" \  
--locations "South Central US"=0 "North Central US"=1 "East US"=2

# WebApp

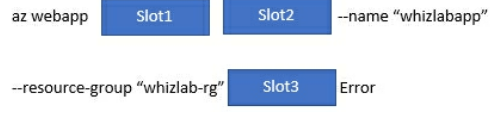
We are creating Docker/Go app to be deployed to Azure App Service Linux  
There’s no resource groups yet  
- az group create  
- az appservice plan create  
- az webapp create

We want to enable App Insights for web app, what needs to be enabled prior to that? **Always on** (???)  
We want web app to stay online always: **Shared tier is no good**, but **basic tier does support Always On** feature (**standard is OK too, but not as cost effective as Basic**)

WebApp has D1 subscription, needs scaling

* Configure web app to use Standard App Service Plan **(we need this. No Shared subscription is enough, but Premium is too much)**
* Enable autoscaling
* Configure scale condition
* Add scale rule

We want a Web App to scale on demand: **Application Insights metric**

We have a web app, we want to stream logs from the app and filter out on any errors:  
  
Slot 1: log  
Slot 2: tail  
Slot 3: --filter

**TODO: AZ LOG TAIL** <https://docs.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs>

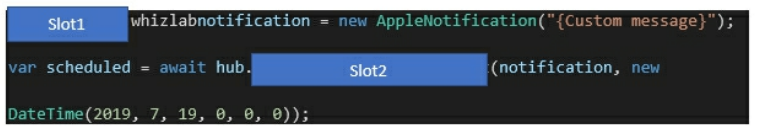
We have a RESTful API backend as Web App  
To secure API, what to configure as **Target? 🡪 HTTPS endpoint**To secure API, what to configure as Gateway **🡪 Client cert**

We have a Web App for 4 customers (they need it on separate, individual instances)

* Ability to automatically scale on demand
* Use deployment slots for staging
* Separate, isolated network
* **Use isolated app service plan**

# Mobile App, Notification Hub

We are communicating with Notification Hubs SDK:



Slot 1: Notification  
Slot 2: ScheduleNotificationAsync

**Todo: SEND notification async vs SCHEDULE notification async**

We have a mobile app that supports offline data sync, update latest messages during normal sync cycles. **Retrieve records from Offline Data Sync using Incremental Sync + Return the updatedAt column from the Mobile Service Backend and implement sorting by using the column**

**TODO: pull/push data sync incremental** <https://docs.microsoft.com/en-us/azure/app-service-mobile/app-service-mobile-offline-data-sync>



Slot1: NotificationHubClient  
Slot2: NotificationHubClient  
Slot3: CreateClientFromConnectionString  
Slot4: SendWindowsNativeNotificationAsync

# App Insights

There’s too much logging done in App Insights: **Implement Application Insights Sampling**Sampling is a feature in [Azure Application Insights](https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview). It is the recommended way to reduce telemetry traffic and storage, while preserving a statistically correct analysis of application data.   
<https://docs.microsoft.com/en-us/azure/azure-monitor/app/sampling>

We have an app using App Insights and we want to set a cap to not go above budget: **Set daily cap for the Application Insights instance**

We have an app with App Insights wired into it:

* We need to know if most customers are progressing through the entire process in the app, or if they are ending the process at some point: **FUNNEL**
* Is page load time impact how many people convert on my page? **IMPACT**
* Analyze how many users return to the app, how often they perform particular tasks or achieve goals: **RETENTION**
* Show how users navigate between pages and feature of the site: **USER FLOWS**

A cohort is a set of users, sessions, events, or operations that have something in common. In Azure Application Insights, cohorts are defined by an analytics query. In cases where you have to analyze a specific set of users or events repeatedly, cohorts can give you more flexibility to express exactly the set you’re interested in.

We are adding app insights logging (**make sure that log messages can be correlated to events tracked by App Insights**):  


Slot1: ApplicationInsightsLoggerOptions  
Slot2: IncludeEventId  
Slot3: app.ApplicationServices

# API Management

We are setting up API management in Azure, authentication via client certificates  
- **INSTALL THE CERTIFICATE INTO API MANAGEMENT**do not: create client certi within API management instance, or add the certi’s data to API management instance, or enable SSL on the API management instance  
  
What policies needs to be used to define the client certificate authentication attribute? **INBOUND** (not primary)

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

we have an API Management instance, app accepts JSON data  
We have external partner connecting to it, data is sent in XML  
We have to ensure that data gets converted from XML to JSON: **use API management policy** (wrong answer: Event Hub namespace, this is used to log events from API management instance)

We have API Management, which must:  
- Support alternative input parameters  
- Remove formatting text from responses: **OUTBOUND Policy**  
- Provide additional context to backend services  
- Rewrite the request URL to match to the format expected by other web service: **INBOUND Policy  
-** Forward the user ID associated with the subscription key for the original request to the backend service: **INBOUND Policy**

**TODO:** <https://docs.microsoft.com/en-us/azure/api-management/api-management-transformation-policies>

We are caching with Azure API Management:

* A set-variable policy to store the detected user identity: **Inbound policy**
* A cache-lookup-value policy: **Inbound policy**
* A cache-store-value policy: **Outbound policy**
* A find-and-replace policy to update the response body with the user profile info: **Inbound policy**

# CDN

Order CDN

1. User requests image from CDN URL, the DNS routes the request to the best performing Point of Presence location
2. If no edge server in the Point of Presence has an imagine in the cache, it will request it from the origin server
3. The origin server will return an image to the Edge server in the Point of Presence (it’ll cache the image and return the image to the user)
4. Subsequent s may redirected to the same Point of Presence

CDN service: if users make requests based on passing an ID parameter, then those should be always served from a Point of Presence, eg https://skillcertlabs.com/Customer.aspx?ID=1

What to set for query string setting of CDN? **Cache every unique URL  
todo** <https://docs.microsoft.com/en-us/azure/cdn/cdn-query-string>

# Logic Apps

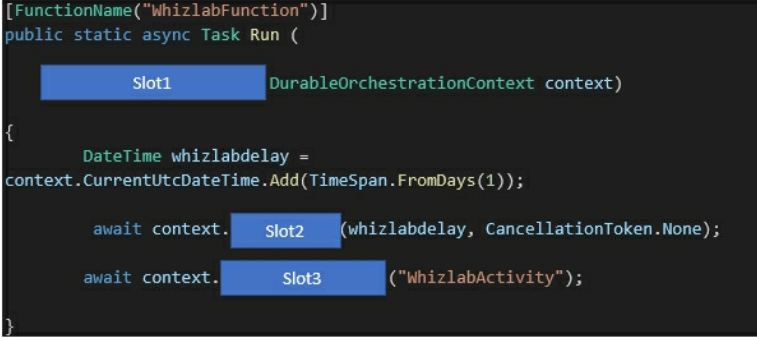
Logic apps: edit B2B workflow, what to use 🡪 Enterprise Integration Pack  
Logic apps: edit definitions in JSON, what to use 🡪 Code View editor  
Logic apps: visually add functionality, what to use 🡪 Logic Apps Designer

We have an Azure Logic App not working:  
**DO: Review the run history, review the trigger history  
DON’T: Review the API connections, review the activity log**

# Function Apps

Ensure that Azure Function writes to Azure Table storage: **use an output binding**

We have a couple apps as Functions, we want to enable App Insights for them  
Where to add instrumentation key? **App settings in Azure Functions**Config amount of telemetry items sent per sec, where to do this? **Host.json**

We are working with Durable Functions, create a durable timer function:  
  
Slot 1: **OrchestrationTrigger** cause when working with durable functions, we use orchestration trigger  
Slot 2: **CreateTimer**  
Slot 3: **CallActivityAsync**

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

We have an Azure Function which reads messages from queue, write data to Table storage



Slot 1: in  
Slot 2: table  
Slot 3: out

# Web Jobs

* **Triggered**: manually/on schedule, runs on single instance that Azure selects for load balancing (no remote debugging)
* **Continous**: starts immediately after creation (endless loop), runs on all instances that the web app runs on (can be restricted to a single instance) (yes remote debugging)

# Event Grid

We are integrating modules of app with Event Grid, they have to filter events  
- Endpoint A: receive failure messages for any resource deployed to Azure subscription: **use filter option EVENTTYPES**  
- Endpoint B: receive messages whenever objects are added to specific container in Blob storage: **Subject beings with or ends with**  
- Endpoint C: receive messages whenever data fields in the message has the value of ‘Org’: **Advanced fields and operators**

<https://docs.microsoft.com/en-us/azure/event-grid/event-filtering>

Todo: refresh on Azure AD + Event Grid (topics vs subscriptions)

* Eg: sign in and sign outs need their separate topics
* SqlFilter
* CorrelationFilter
* True/FalseFilter
* No Filter: <https://docs.microsoft.com/en-us/azure/service-bus-messaging/topic-filters>

Recheck questions 77-

Parsing event data from Event grid:



Slot1: id  
Slot2: topic  
Slot3: eventType

# Event Hub

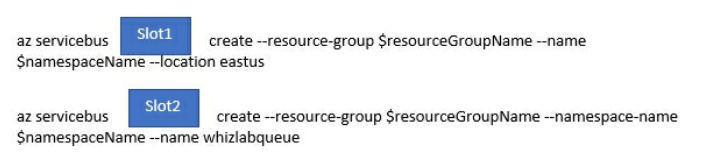
We are interacting with Event Hub: we want high throughput, what API to use? **CreateBatch**

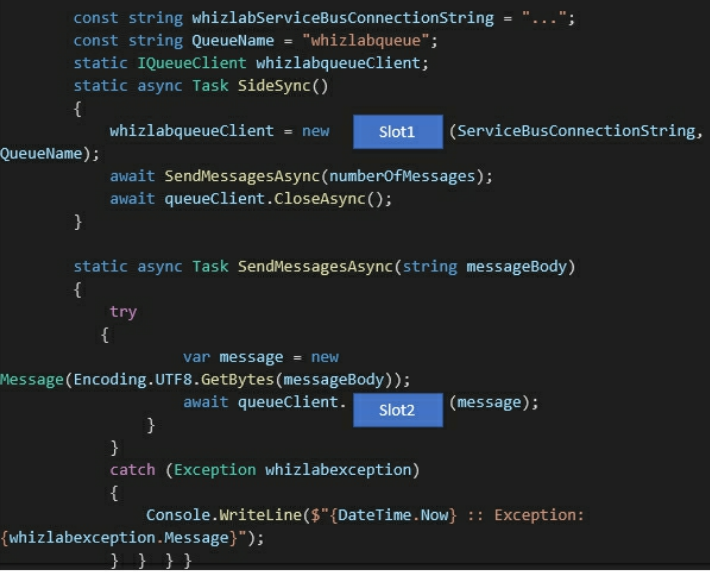
<https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-programming-guide>

Then use **SendAsync**

Event Hub, data is streamed to BLOB storage  
**Use Event Hubs Capture**<https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-capture-enable-through-portal>

# Service Bus

We are creating Azure Service Bus queue  
  
Slot 1: namespace  
Slot 2: queue

We have an app that needs to interact with Azure Service bus queue  
  
Slot 1: QueueClient  
Slot 2: SendAsync

We are creating a service bus in namespace “skillcertlabs”  
New-**AzureRmServiceBusQueue** -ResourceGroupName ""skillcertlabs-rg"" -**NamespaceName** skillcertlabs -Name skillcertlabsqueue -EnablePartitioning $False"

We have an app:

* Driver selects restaurant for which they will deliver order
* Orders are sent to all drivers in the area
  + But only orders for selected restaurant will get shown to drivers
  + First driver who accepts it, makes it disappears for others
* We are using Azure Service Bus

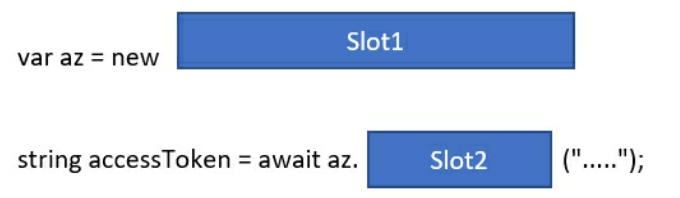
**CREATE A SINGLE SERVICE BUS Topic  
CREATE A SINGLE SERVICE BUS Namespace  
CREATE A SERVICE BUS Subscription for each restaurant for which a driver can receive messages**

Drivers are subscribers

# Security

Where to store client certificates: **HTTP request header** (not client cookie, http message body or url query string)  
What encoding to use? **Base64**

We have a managed service identity, we want GetCredentials to access token via it:

  
Slot 1: Azure**ServiceTokenProvider**() <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-to-use-vm-token>  
Slot 2: GetAccessTokenAsync

Multi factor authentication for Azure AD:

* Needs Azure AD Premium
* Azure Ad 🡪 create new conditional access policy

Authentication:

* To communicate with MS Support: **Microsoft.Support/\***
* Useful:
  + Get-AzRoleDefinition –Name „Reader” | ConverTo-Json Out-File c:\sample.json
  + Set-AzRoleDefinition –Role $role
  + (there’s no update)

The user’s Security Pin must be stored in such a way that access to the database does not allow the viewing of Security Pins. The web application is the only system that should have access to Security Pins.

**NO:** “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”  
*Data Masking is normally used when you want to mask certain parts of a column data value. Here we need to ensure that the Security PIN cannot be deciphered at all.*

**NO:** “Enable Always Encrypted for the SecurityPin column using a certificate based on a trusted certificate authority. Ensure users are given instructions to ensure that the certificate is installed on user machines”

**YES:** “Enable Always Encrypted for the SecurityPin column using a certificate contained in Azure Key Vault and grant the WebAppldentity service principal access to the certificate”

We have an app secured by using AAD account (which has full access to all namespaced of the AKS cluster) 🡪 **Place the AAD account into an Azure AD group, create a ClusterRoleBinding and assign it to the group**