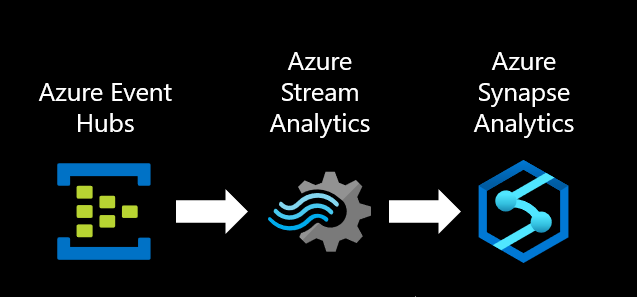
**Azure Stream Analytics High throughput ingestion to dedicated SQL pool**

## Pre-requisite:

|  |  |  |  |
| --- | --- | --- | --- |
| No | Pre-requisite | Example resource name | Reference Link/compute details |
| 1 | Provision Azure Synapse workspace | <azsynapsews1> | <https://docs.microsoft.com/en-us/azure/synapse-analytics/get-started-create-workspace> |
| 2 | Provision SQL pool | SQLPool1 | <https://docs.microsoft.com/en-us/azure/synapse-analytics/quickstart-create-sql-pool-portal> |
| 3 | Provision Spark pool | SparkPool1 | <https://docs.microsoft.com/en-us/azure/synapse-analytics/quickstart-create-apache-spark-pool-portal> |



|  |  |
| --- | --- |
| Instructions | Reference Link/ Comment |
| Create an Event Hub input | <https://docs.microsoft.com/en-us/azure/stream-analytics/stream-analytics-real-time-fraud-detection?toc=/azure/synapse-analytics/sql-data-warehouse/toc.json&bc=/azure/synapse-analytics/sql-data-warehouse/breadcrumb/toc.json#create-an-azure-event-hubs-to-ingest-events> |
| Configure and start event generator application   1. Download the zip file for the Event Generator app 2. Use it on your system or copy it into an Azure VM, preferably in the same region, and unpack zip file. 3. Update **SensorEventGenerator.exe.config** 4. Open PowerShell in that folder and run **InvokeSenders.ps1** script | [https://github.com/chetanmsft/utilities/releases/tag/v1.0](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgithub.com%2Fchetanmsft%2Futilities%2Freleases%2Ftag%2Fv1.0&data=02%7C01%7CPriyanka.Langade%40microsoft.com%7Cef29cb911f4e4850e1b608d829ca7591%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637305296813231398&sdata=oCfUDzhcMf9EB99gV1eTsRhV05pBl7QSHWYzsCYeoLo%3D&reserved=0)    To configure an event hub with the Event Generator app:  In the **SensorEventGenerator.exe.config** file update the items highlighted below.    <!-- Service Bus specific app settings for messaging connections -->  <add key="EventHubName" value="<Provide Name of Event Hub>"/>  <add key=" EventHubConnectionString " value="<Provide Connection string-primary key>"/>  </appSettings> |
| Provision a Stream Analytics job | <https://docs.microsoft.com/en-us/azure/stream-analytics/stream-analytics-real-time-fraud-detection?toc=/azure/synapse-analytics/sql-data-warehouse/toc.json&bc=/azure/synapse-analytics/sql-data-warehouse/breadcrumb/toc.json#create-a-stream-analytics-job-to-manage-streaming-data> |
| Specify job input |  |
| Create Tables in dedicated SQL pool | Execute Script on dedicated SQL pool to create tables.  ./Develop/ 01 Create Streaming Tables |
| Specify Outputs:   1. dwgranular 2. dwaggregate   For each output (dwgranualr and dwaggregate):   1. select database name, 2. provide table name created for Streaming job in dedicated SQL pool, 3. username, 4. password |  |
| Specify Query for output to dwaggregate:  From **Job topology** >> **Query**, add SQL script in | Refer script: ./Develop/00 Streaming Query to Aggregate |
| Click **Start** to stream the analytics job. |  |
| From a dedicated SQL pool, showcase the high throughput egress to Synapse. | Execute Script on dedicated SQL pool to show streaming ingestion.  ./Develop/ 02 Streaming ingestion to SQL Pool |
| Stop PowerShell script and Stop Streaming job |  |

Note: You can also follow instructions for an end-to-end example here: [Use Azure Stream Analytics with Azure Synapse Analytics](https://docs.microsoft.com/en-us/azure/stream-analytics/stream-analytics-real-time-fraud-detection?toc=/azure/synapse-analytics/sql-data-warehouse/toc.json&bc=/azure/synapse-analytics/sql-data-warehouse/breadcrumb/toc.json" \l "scenario-telecommunications-and-sim-fraud-detection-in-real-time)