**Synapse Assessment Tool**

**User Manual**

**1.1 Prerequisites**

**Operating System** : Windows 10 or above

**Tools** : Microsoft Excel (Office 365) – To view output file,

WinRAR – To extract the zip file

**1.2 Software Installation Steps**

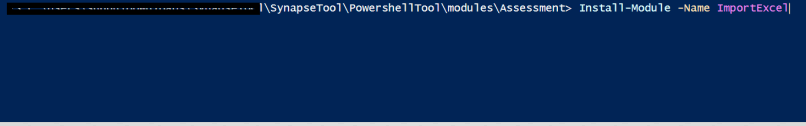
* To run the Synapse Assessment tool,
* We need to follow the below steps to make sure the tool is running properly.

Step 1:

* Open **PowerShell** as Administrator mode(Refer the screenshot) and run the following commands:



* Install-Module -Name ImportExcel
* Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass, select Yes to All
* Install-Module -Name SqlServer -Scope CurrentUser



Step 2:

Download the zip file (**SynapseTool.zip**) from the Github repository and save and extract it using **WinRAR software** and place the files in your system.

Graphical user interface, application

Description automatically generated

* Open the **config.json** fileunderthe below folder path, **SynapseTool>PowershellTool>modules>Assessment**

Graphical user interface, text, application

Description automatically generated

**Below are the key properties in the config json file,**

**1.1.1 ServerName:**

Enter the ServerName here (example “workbenchproductionsqlserver”)

**1.1.2 IntegratedSecurity:**

If IntegratedSecurity is set to “0” or “1”: In Windows Powershell ISE, when we start RunAssessment DB credentials (User Name and Password) are mandatory.

If IntegratedSecurity is set to “Yes” or “No”: In Windows Powershell ISE, when we start RunAssessment DB credentials (User Name and Password) are not mandatory.

**1.1.3 ConfigFileName:**

User should enter the configFileName here (Example: “cs\_dirs.csv”)

**1.1.4 ExtractSPDetails:**

When “ExtractSPDetails” is set to ‘0’- the Synapse tool should skip the Extraction of SP Details for the list of DBs mentioned to scan.

When “ExtractSPDetails” is set to ‘1’- the Synapse tool should start Extracting the SP Details for the list of DBs mentioned to scan.

**1.1.5 SkipExtraction:**

When “SkipExtraction” is set to ‘0’- the Synapse tool should skip the entire Extraction (SP Details, SchemaSummary, Table details, View details, Assessment Report and Assessment Summary) for the list of DBs mentioned to scan.

When “SkipExtraction” is set to ‘1’- the Synapse tool should start Extracting (SP Details, SchemaSummary, Table details, View details, Assessment Report and Assessment Summary) for the list of DBs mentioned to scan.

**1.1.6 SkipInputFolderClenup:**

When “SkipInputFolderCleanup” is set to ‘0’ it will clean up the Input folder completely.

When “SkipInputFolderCleanup” is set to ‘1’ it will skip the clean-up activity for the Input folder.

**1.1.7 SkipAssessment:**

When “SkipAssessment” is set to ‘0’ it will extract the following details (Database Name, SQLObjectType, FileName, Line Number, FailedText, Category, Reason and Recommendation) to Assessment Report and Pivot table into Assessment Summary sheet in InvestmentandAssessmentReport.xlsx.

**1.1.8 SkipInventeryCollection**

“SkipInventeryCollection” to ‘0’

**1.1.9 “ListOfDBsToScan”:**

Enter all the Database name to be Scanned with comma separated here (Example: DB1, DB2, DB4)

**1.1.10 “ListOfDBsToSkip”:**

Enter all the Database name with comma separated here (Example: DB3, DB5, DB6) to skip the Scanning process using Synapse tool.

**1.1.11 “DefaultDBConnect”:**

Set Default DB to connect as “LOBBY”. It will connect to the Database.

**1.1.12 GenerateLogFileInSameDir:**

Set “GenerateLogFileInSameDir” as ‘1’.

**1.1.13 “RetryFailedDBsMode”:**

Yet to be implemented

**1.3 Tool Execution Steps**

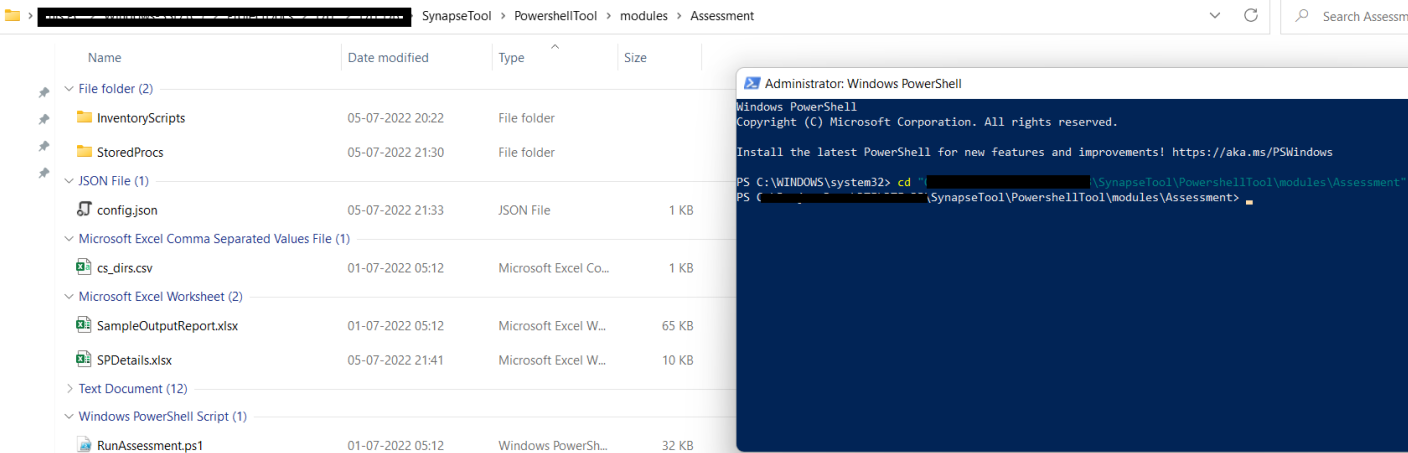
NOTE : This tool can be used to assess both on prem SQL and Azure Cloud SQL databases against Synapse Sql pool.

Text

Description automatically generated

**Step 1:**





Run the following command

**Powershell.exe -File RunAssessment.ps1** in the PowerShell window.

**Step 2:**

This script can be executed in two different modes based on a property called **Integrated Security**,

If this script is triggered in an on prem server, then the Integration Security property should be set to “Yes” as below,

* In case of **windows authentication**, if your SQL instance is available in an on prem machine, please use the below settings in config.json file

If this script is triggered in a local system or the script is intended to run against a cloud SQL server, then the Integration Security property should be set to “0” as below,

* In case of **SQL authentication**, if your SQL instance is available in a cloud environment , please use the below settings in config.json file

Graphical user interface, text

Description automatically generated

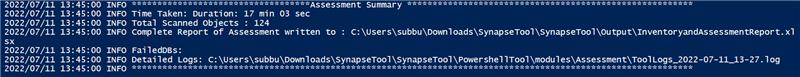
**Graphical user interface, text

Description automatically generated**

Please wait until the script completes its execution. This script may take time to execute.

**Final Output :**

Here is the final output,

****

**Graphical user interface, application, table, Excel

Description automatically generated**

**Graphical user interface, application

Description automatically generated**