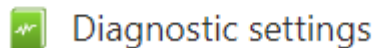
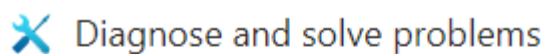


## 😊 Settings Diagnostic Logs for Azure Data Lake

In this process, you're configuring diagnostic logs for Azure Data Lake Storage. The end goal is to enable monitoring and analysis of activities within your storage account, such as file uploads, deletions, and access patterns. By setting up diagnostic logs and analyzing the generated data, you gain insights into how your storage resources are being utilized, which can help optimize performance, troubleshoot issues, and ensure compliance with security and regulatory requirements.

1. Now you need to go to your Storage account and check whether you have two separate accounts or not. If not, then create one.
2. After that get inside of any one of the accounts and search for diagnostic settings.



3. In there you will have multiple services and they are disabled. Now you need to go inside of blob service.

Refresh

Feedback

Subscription \* ⓘ

Azure Pass - Sponsorship

Resource group ⓘ

demo-grp

Resource type ⓘ

Storage accounts

Resource ⓘ

appstorage120

Azure Pass - Sponsorship

>

demo-grp

>

appstorage120

Select any of the resources to view diagnostic settings.

Name	Resource type	Resource group	Diagnostics status
<div><div></div><div>appstorage120</div></div>	Storage account	demo-grp	<div><div></div><div>Disabled</div></div>
<div><div></div><div>blob</div></div>	Storage account	demo-grp	<div><div></div><div>Disabled</div></div>
<div><div></div><div>queue</div></div>	Storage account	demo-grp	<div><div></div><div>Disabled</div></div>
<div><div></div><div>table</div></div>	Storage account	demo-grp	<div><div></div><div>Disabled</div></div>
<div><div></div><div>file</div></div>	Storage account	demo-grp	<div><div></div><div>Disabled</div></div>

4. Then you have to click on add diagnostic settings

Refresh Feedback

Subscription \* ⓘ Azure Pass - Sponsorship Resource group ⓘ demo-grp Resource type ⓘ Storage accounts Resource ⓘ appstorage120/blob

Azure Pass - Sponsorship > demo-grp > appstorage120/blob

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. [Learn more about diagnostic settings](#)

Diagnostic settings

Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting
------	-----------------	-----------	-------------------------	------------------	--------------

No diagnostic settings defined

[+ Add diagnostic setting](#)

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- Storage Read
- Storage Write
- Storage Delete
- Transaction

- Now you need to choose what you want for the logs and where you want to send them.
- Below we have chosen our logs, and we are sending them to a different storage account.
- After that give it a name and save it.

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name \*

Logs

Category groups ⓘ

☐ audit ☐ allLogs

Categories

☒ Storage Read

☒ Storage Write

☐ Storage Delete

Metrics

☒ Transaction

Destination details

☐ Send to Log Analytics workspace

☒ Archive to a storage account

**i** Showing only general-purpose v2 storage account

Location  
North Europe

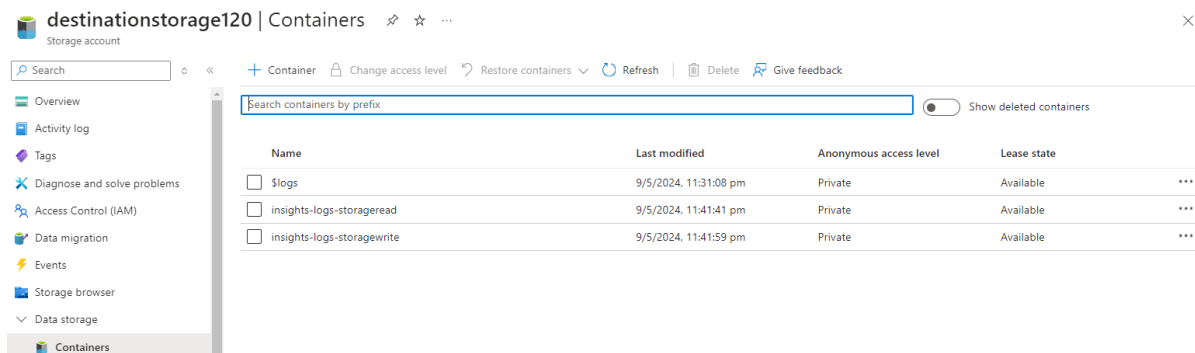
Subscription  
Azure Pass - Sponsorship

Storage account \*  
destinationstorage120

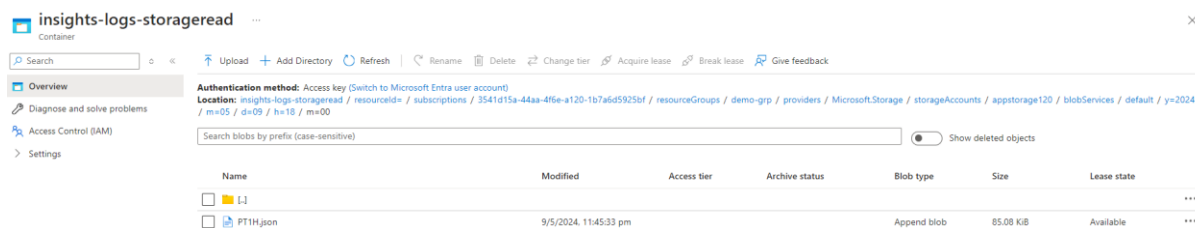
☐ Stream to an event hub

☐ Send to partner solution

- Now it will generate data based on read write and transactions.
- What we need to do is perform as many tasks in our storage as we can.
- Like creating containers, uploading files into them or creating a directory.
- Just perform as many tasks as you can because it will take time to generate the data.
- After 5-10 minutes if you go inside of the storage account which was the destination for our diagnostic data then you will find two storage accounts.

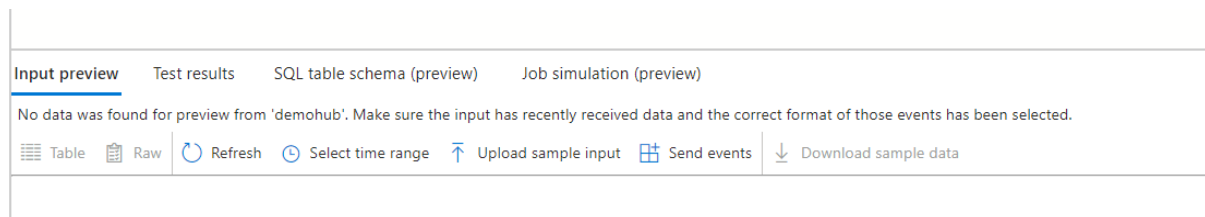


13. Then if you go inside of the container you will see that we have multiple layers of folders, then after in the last we got our JSON file in the form of diagnostic information for this hour.



14. Now you need to download this and directly move to stream analytics and open query in there.


15. And inside of the query you will find that you have the option to upload the sample data.



16. Now you need to click on upload and upload the sample file here.

## Upload sample data

Upload sample data from file \*

"insights-metrics-sample.json" 

You can upload a file with sample input to test your query against. Stream Analytics supports processing input in JSON, CSV and Avro formats with UTF-8 encoding natively.

17. Then effective immediately you will get the raw data in tabular format.

Showing data from uploaded file 'insights-metrics-sample.json'.

View in JSON

Table

Raw

Reset

Upload sample input

Send events

Download sample data

count <i>bigint</i>	total <i>bigint</i>	minimum <i>bigint</i>	maximum <i>bigint</i>	resourceId <i>string</i>	time <i>datetime</i>	metricName <i>string</i>
2	2	1	1	"/SUBSCRIPTIONS/691...	"2023-05-18T07:00:00...."	"Transactions"
13	13	1	1	"/SUBSCRIPTIONS/691...	"2023-05-18T07:02:00...."	"Transactions"
3	3	1	1	"/SUBSCRIPTIONS/691...	"2023-05-18T07:02:00...."	"Transactions"
7	7	1	1	"/SUBSCRIPTIONS/691...	"2023-05-18T07:00:00...."	"Transactions"
3	3	1	1	"/SUBSCRIPTIONS/691...	"2023-05-18T07:02:00...."	"Transactions"
1	1	1	1	"/SUBSCRIPTIONS/691...	"2023-05-18T07:02:00...."	"Transactions"
13	13	1	1	"/SUBSCRIPTIONS/691...	"2023-05-18T07:00:00...."	"Transactions"
17	17	1	1	"/SUBSCRIPTIONS/691...	"2023-05-18T07:02:00...."	"Transactions"