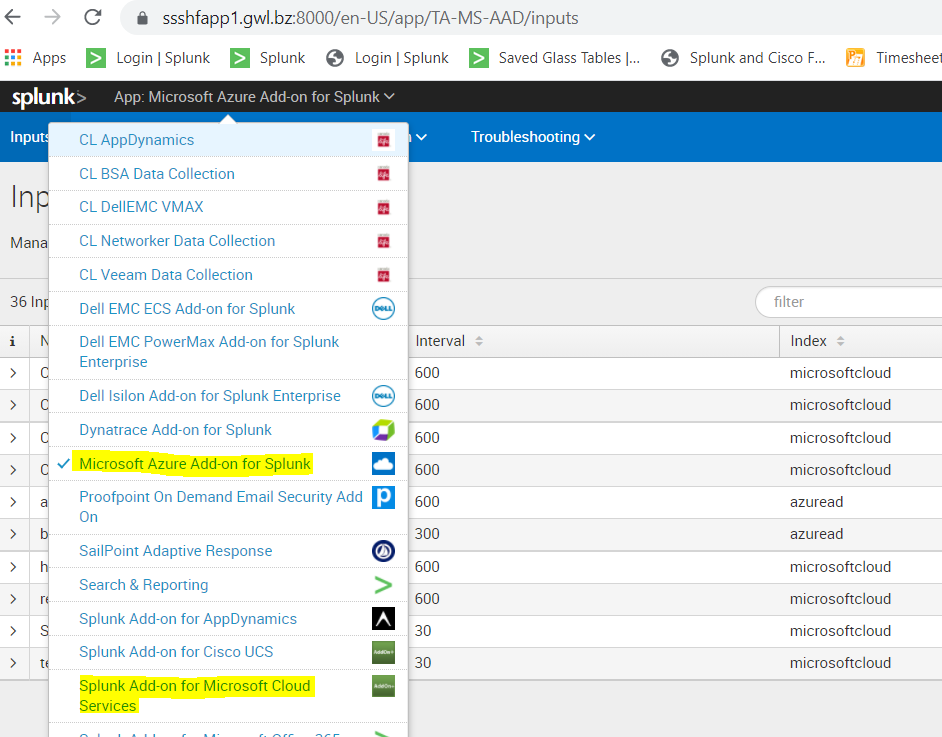
All the inputs related to Azure are configured in SSSHFAPP1 standalone Heavy Forwarder.

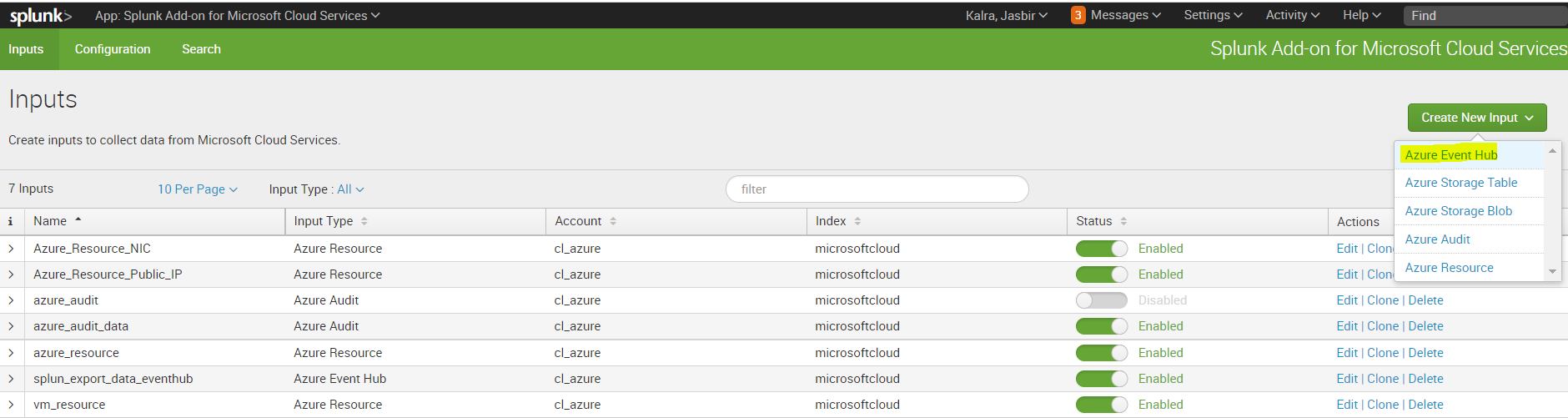
Addons used are:

1. Microsoft Azure Add-on for splunk
2. Splunk Add-on for Microsoft Cloud Service

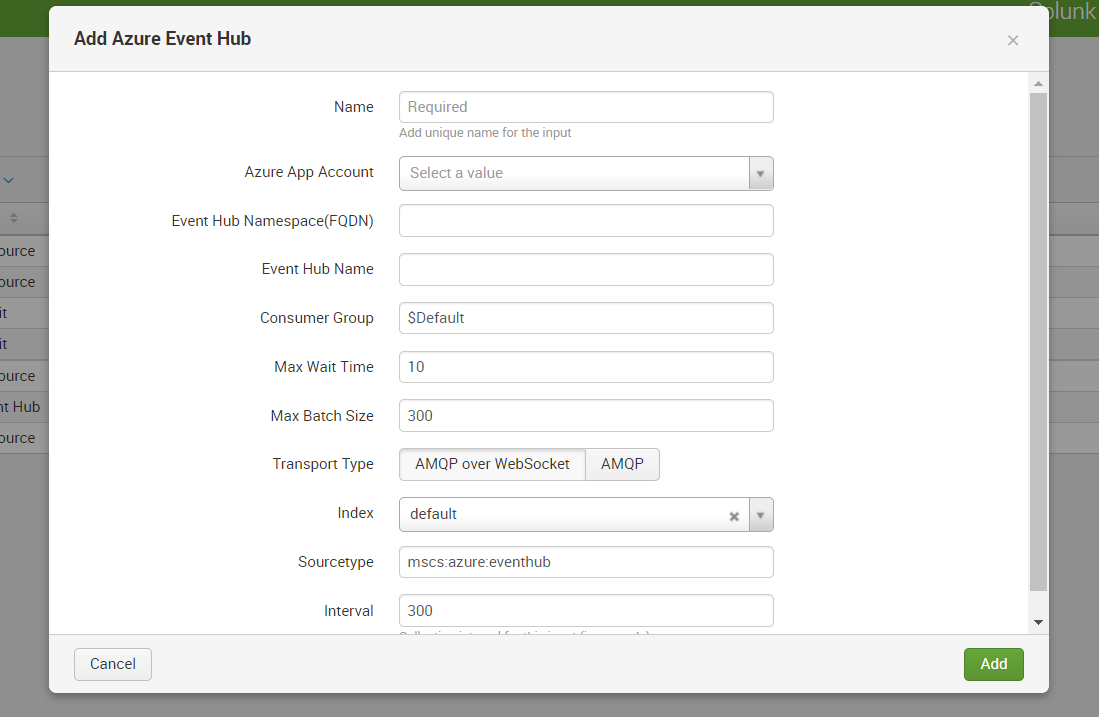


* EventHub Configuration

1. Add-on used for EventHub Configuration is Splunk Add-on for Microsoft Cloud Services
2. To configure go to Splunk Add-on for Microsoft Cloud Services >> inputs
3. Click on create new input >> Azure Event Hub



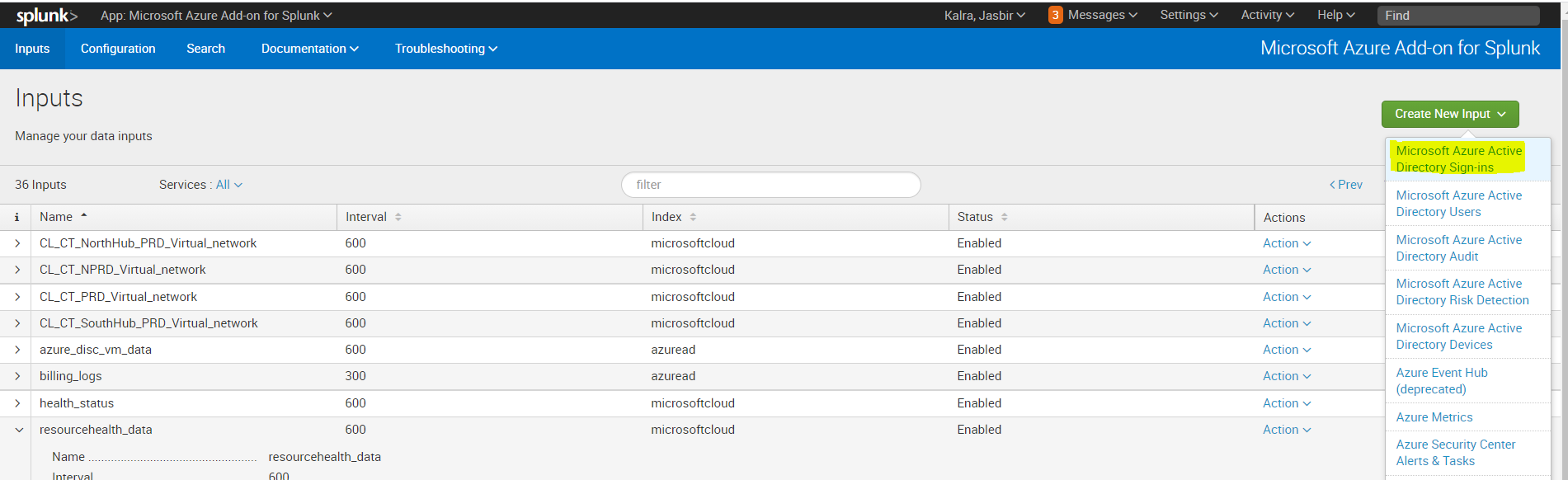
1. In the config page please add below details



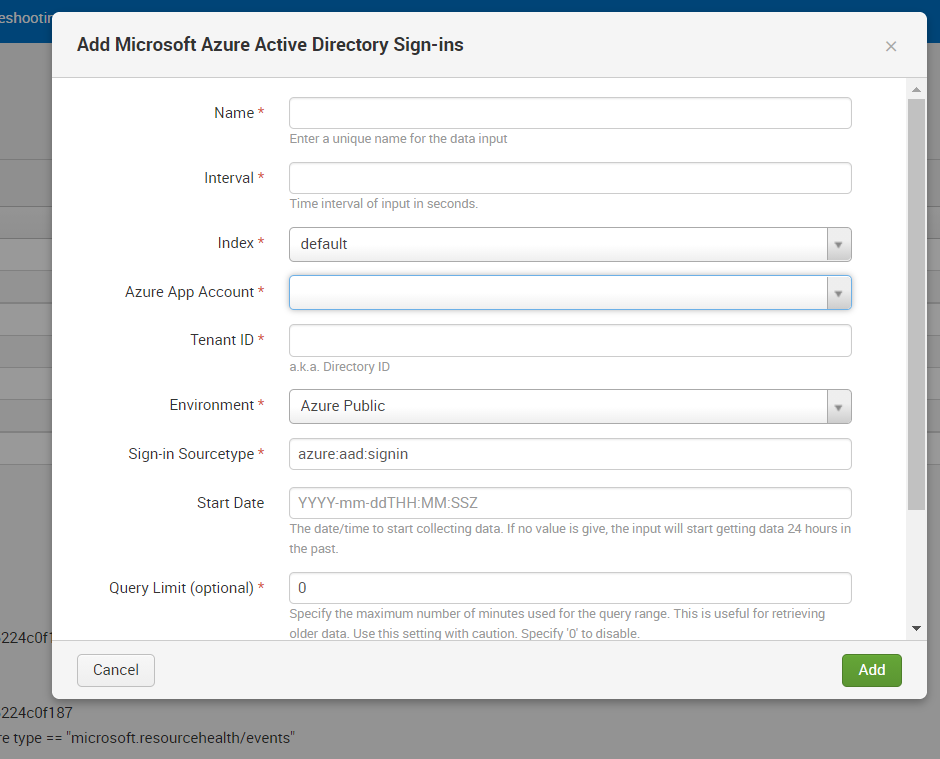
* + - Name: input name according to request.
    - Azure App Account: please select azure account in which event hub is created.
    - Event Hub namespace: it can be found on azure site under that EventHub.
    - Index: we can select as per requirement.
    - Rest all can be default.

1. Click on add. And we should be able to get data in splunk from EventHub.

* Azure API Configs
  1. Add-on used for azure api configs is Microsoft Azure Add-on for splunk
  2. To configure go to is Microsoft Azure Add-on for splunk >> inputs >> create new input
  3. For example, we want to get sign in data click on Microsoft Azure Active Directory sign ins

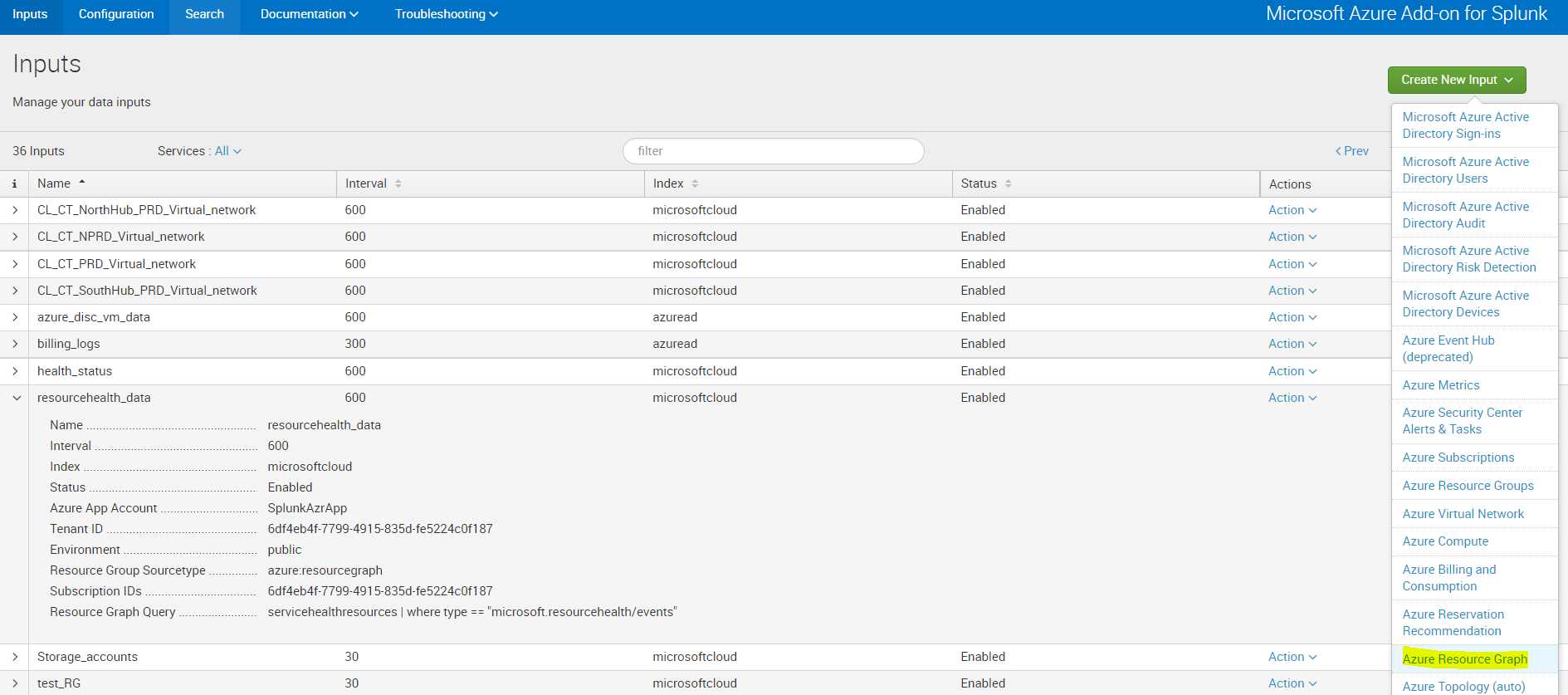


* 1. In config page fill all necessary details as below

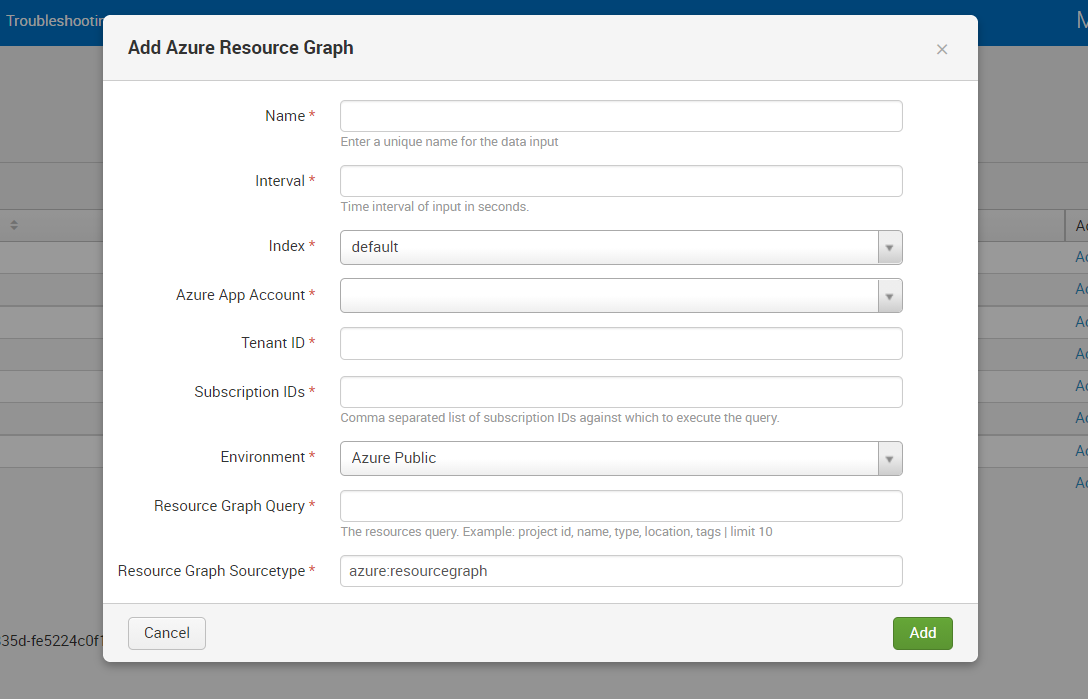


* + - * Name : give input name
      * Interval : at what interval input should run mention that
      * Index: select appropriate index
      * Azure Ap Account: select azure account of which sign in logs need to be ingested
      * Tenant ID: please enter tenant id
      * Rest we cam keep as default.
  1. Click on Add. Data should be coming into splunk.
* Azure Resource Graph Queries Configuration

1. Add-on used for azure api configs is Microsoft Azure Add-on for splunk
2. To configure go to is Microsoft Azure Add-on for splunk >> inputs >> create new input
3. Select Azure Resoure Graph option from the list



1. In Config page fill all necessary details as below



* + - Name: give input name
    - Interval: at what interval input should run mention that
    - Index: select index as per requirement
    - Azure App Account: select an azure account
    - Tenant ID: enter Tenant ID
    - Subscription ID’s: enter subscription ID on which resource graph query will run.
    - Resource Graph Query: here query needs to be added which can be get from azure portal as per requirement.
    - Rest all can be used as default.

1. Click on Add. Data should start coming into splunk.
2. For this resourcehealth\_input can be referred which is on SSSHFAPP1.

* Using all data custom dashboard is created. Please refer below url:

https://splunk.gwl.bz/en-US/app/microsoft\_azure/Custom\_Dashboards?form.field1.earliest=-24h%40h&form.field1.latest=now