NetBrain Single Pane of Glass (SPoG) Integration_Splunk

NetBrain applicable versions: 7.1a1, 8.0

Contents

Instruction

What is NetBrain Single Pane of Glass (SPoG)?

NetBrain integrates with different data sources within an enterprise to use NetBrain map and Qapp for data correlation, analysis, and troubleshooting.

How does NetBrain SPoG work?

NetBrain has Python function defined in API Plugin to send HTTP/HTTPS request to 3rd party system to query 3rd party system data via REST API. End user needs to specify the 3rd party system REST API for certain corresponding data in NetBrain API Parser. NetBrain will then be able to implement the parser in a Qapp to further process the REST API retrieved data to generate NetBrain Data View on NetBrain maps.

Integrate with Splunk

In this case, we mainly focus on calling Splunk REST API and set Splunk searchquery as an input to retreive corresponding data from Splunk, then put the data into NetBrain system with correlation, analysis or troubleshooting. First, customer needs to know how to use Splunk REST API, click here.

Splunk REST API

Splunk provides an API method for every feature in our product. Programmers can use our API to make their own applications, phone apps, widgets, and other projects that interact with Splunk®. Programs talk to the Splunk API over HTTP, the same protocol that your web browser uses to interact with web pages and conforms to the principles of Representational State Transfer (REST).

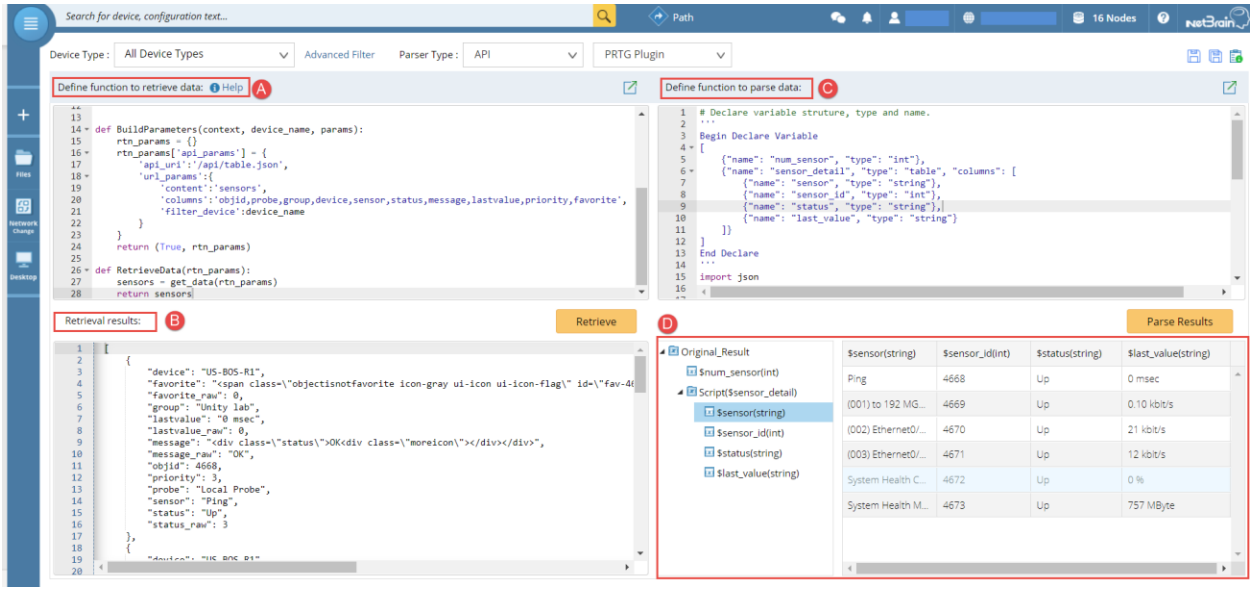
Second, to define NetBrain API Parser, end user needs to also understand how to use the Splunk search query, click here.

Splunk Search App

The Search app, the short name for the Search & Reporting app, is the primary way you navigate the data in your Splunk deployment. The Search app consists of a web-based interface (Splunk Web), a command line interface (CLI), and the Splunk SPL.

After customer confirm that the syntax of search query is correct and can retrieve the expecting data from Splunk console then we can forward to the next step **Create API Plugin in NetBrain for Splunk**.

Create NetBrain API Parser



A. Define retrieve data function
    a. Customize Python functions:
        i. BuildParameters()
        Define Splunk HTTP API parameters.
            - api_url: Splunk API HTTP URI without host server domain name section
            - url_params: Splunk API HTTP Query parameters(Splunk search query)
        ii. RetrieveData()
        Call API Plugin Python function to retrieve data via REST API
B. Review retrieved data
C. Define parse data function
D. Review parsed data

Define NetBrain API Plugin

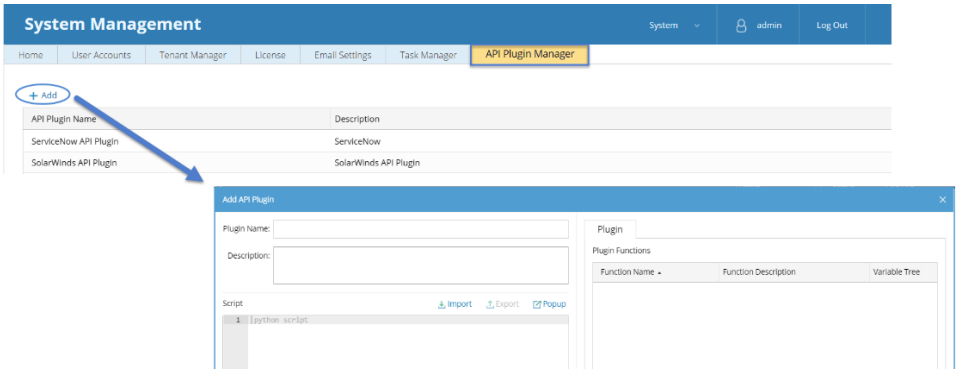
API Plugin is a component to define a function template for the API Parser and API Server to work with a third-party system.

To define a new API plugin, complete the following steps.

Tip: The system provides a built-in Splunk API Plugin and you can refer to it to write your own ones in the API Plugin Manager.

At the beginning, customer needs to know how to creating searches using the Splunk REST API, click here.

Step:
1. Log into System Management page.
2. Select the API Plugin Manager tab and click Add.



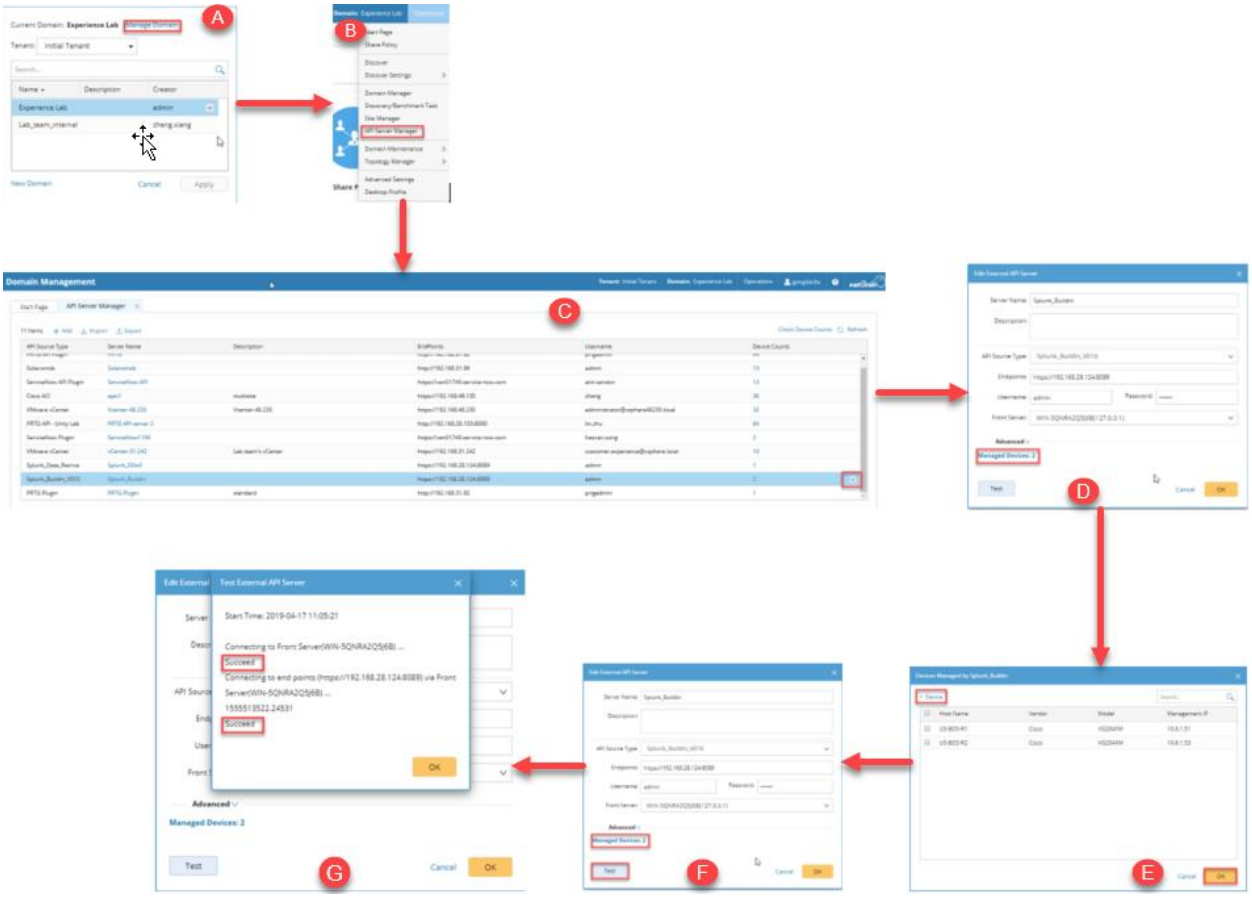
3. Enter a name in the Plugin Name field, such as Splunk Incidents.
4. Enter a description of the API plugin in the Description field.
5. Enter the API script in the Script field.

   Tip: You can click Popup to prompt a larger script interface. Alternatively, you can click Import to import an existing python file directly.
6. Click Save to save the definition.

Test NetBrain API Server Instance Connectivity to Splunk Instance

Adding an External API Server

Customer needs to navigate to NetBrain **Domain Management** then **API Server Manager** to set the API plugin to corresponding devices. Steps showing below:



A) Click the domain name on right up corner of customer NetBrain desktop, click on the **Manage Domain**.
B) After redirection into **Domain Management** page, click on **Operations** and select **API Server Manager**.
C) Find the plugin customer just created, to the right end of current row click the small arrow and select **Edit**.
D) Fill in all fields in the new open dialog, click on **Manage Devices**.

Note: customer must input the Splunk account information correctly (username, password and endpoint).
E) In the new open dialog, choose devices to connect to Splunk plugin, click **OK**.
F) Then after jump to the previous dialog, click on the **Test** button.
G) Check the test result.

If the test result is **failed** then customer needs to check the NetBrain front server apilog file to confirm what kind of error has been occurred.

Create NetBrain Qapp with NetBrain API Parser

General NetBrain Data View by NetBrain Qapp

Appendix

NetBrain API Plugin Code Standard

1. To easily maintain and scale API Parser Library in the future, only extract parameters passed from Parser. DO NOT hard code any REST API HTTP parameters in API Plugin Python functions.
2. To prevent more HTTP request sending from NetBrain to 3rd party systems, use Basic Authentication for HTTP calls as long as 3rd party system supports Basic Auth.
3. To easily organize HTTP call parameters, return the following 4 values to get_data() function:
    a. endpoint: 3rd party system host address, which is defined in API Server Manager
    b. username: 3rd party system login username to be used by HTTP call, which is defined in API Server Manager
    c. password: 3rd party system login password to be used by HTTP call, which is defined in API Server Manager
    d. api_params: HTTP request parameters defined in API Parser
4. To simplify the output in API Server Manager Test result, trim the sample REST API call result as much as possible in _test() function.

NetBrain API Parser Code Standard

1. Define HTTP request parameters in BuildParameters() function by following the Python dictionary structure below:

```
rtn_params['api_params'] = {
  'api_uri':'/api/table.json',
  'url_params':{
    'content':'sensors',
```

```
            'columns':'objid,probe,group,device,sensor,status,message,lastvalue,priority,favorite',
            'filter_device':device_name
        }
    }
```

2. Trim the result by better defining the query parameters, instead of further process the returned result later in NetBrain parser.
3. Implement the main logics by calling API Plugin functions in RetrieveData() function