CloudHub Logs to Splunk

**High level reference guide**

|  |  |
| --- | --- |
| **Author**: | Sabu Sree Raj Somarajan |
| **Date**: | 03.10.2017 |
| **Version**: | 1.0 |
| **State**: | Released |

**Updates**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Reviewer** | **Comments** |
|  |  |  |  |

Table of Contents

[1 Document Control 2](#_Toc494973574)

[1.1 Document Purpose 2](#_Toc494973575)

[1.2 Document Scope 2](#_Toc494973576)

[2 Solution Context 3](#_Toc494973577)

[2.1 Problem 3](#_Toc494973578)

[2.1.1 Logs beyond the default threshold 3](#_Toc494973579)

[2.1.2 Logs beyond delete 3](#_Toc494973580)

[3 Solution 4](#_Toc494973581)

[3.1 Splunk Log Aggregator 4](#_Toc494973582)

[3.1.1 Steps 4](#_Toc494973583)

[3.1.2 Pros 8](#_Toc494973584)

[3.1.3 Cons 8](#_Toc494973585)

[3.1.4 Sample project 8](#_Toc494973586)

[3.2 Splunk Log4j Appender 8](#_Toc494973587)

[3.2.1 Steps 8](#_Toc494973588)

[3.2.2 Pros 9](#_Toc494973589)

[3.2.3 Cons 9](#_Toc494973590)

# Document Control

## Document Purpose

This document could be used as a high level reference guide for publishing mule application logs to [Spulnk](https://www.splunk.com/).

## Document Scope

This document covers general methods of retrieving logs from CloudHub, and is not a detailed implementation manual or complete guide for individual use cases, or a tutorial on how to publish mule logs to Splunk.

# Solution Context

## Problem

CloudHub’s log persistence is limited in terms of size and log availability period, and organizations often need to access logs beyond these thresholds, or sometimes would want to publish the logs to an external service like Splunk.

For more details on logging in Mule: <https://docs.mulesoft.com/mule-user-guide/v/3.8/logging-in-mule>

### Logs beyond the default threshold

CloudHub stores logs of up to 100 MB per app & per worker or for up to 30 days, whichever limit is hit first. See [https://docs.mulesoft.com/runtime-manager/viewing-log-data - about-log-persistence](https://docs.mulesoft.com/runtime-manager/viewing-log-data#about-log-persistence)

### Logs beyond delete

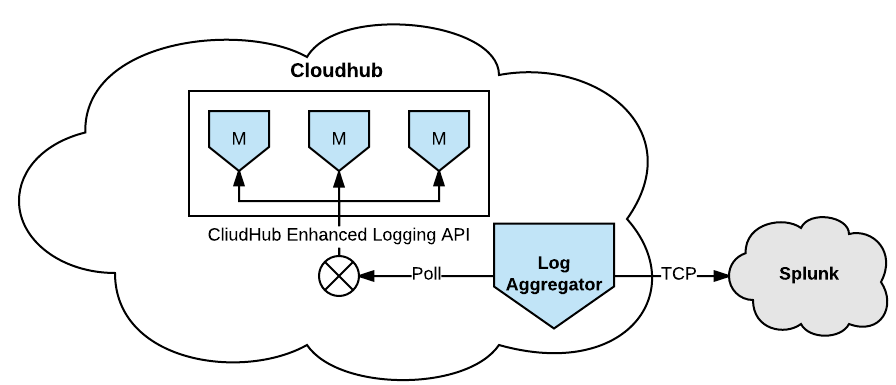


# Solution

These are the two main ways of publishing CloudHub application logs to Splunk.

## Splunk Log Aggregator

The idea is to create an independent mule application that retrieves the CloudHub logs using the [CloudHub Enhanced Logging API](https://anypoint.mulesoft.com/apiplatform/anypoint-platform/#/portals/organizations/68ef9520-24e9-4cf2-b2f5-620025690913/apis/34348/versions/35742), and publishes them to Splunk using their TCP API or HTTP API at regular intervals.



### Steps

Here is a deep dive into the overall application logic taken from MuleSoft’s support article.

|  |
| --- |
| **See API documentation for Anypoint Platform Access Management:** [**https://anypoint.mulesoft.com/apiplatform/anypoint-platform - /portals/organizations/68ef9520-24e9-4cf2-b2f5-620025690913/apis/11270/versions/11646/pages/60046**](https://anypoint.mulesoft.com/apiplatform/anypoint-platform#/portals/organizations/68ef9520-24e9-4cf2-b2f5-620025690913/apis/11270/versions/11646/pages/60046) |
| **See API documentation for CloudHub Enhanced Logging API:** [**https://anypoint.mulesoft.com/apiplatform/anypoint-platform/ - /portals/organizations/68ef9520-24e9-4cf2-b2f5-620025690913/apis/34348/versions/35742**](https://anypoint.mulesoft.com/apiplatform/anypoint-platform/#/portals/organizations/68ef9520-24e9-4cf2-b2f5-620025690913/apis/34348/versions/35742) |

1. Define the frequency to retrieve application/s logs from CloudHub
   1. Define a Poll component as the Input of the main flow with a Fixed Frequency schedule
2. Generate the access token: See [Generate Authorization Bearer Token for Anypoint Platform](#_Generate_Authorization_Bearer_1)
3. Specify the application(s)
   1. The application domain can be hardcoded in the Splunk log aggregator logic if there is only one application.
   2. For multiple application logs, see [Retrieve Applications List](#_Retrieve_Applications_List_1)
4. For each application, fetch the log records: See [Retrieve Application Logs](#_Retrieve_Application_Logs)
5. Save the last retrieved **recordId** so that only new records are fetched during the next iteration
6. Publish the log records to Splunk. A Splunk Enterprise TCP input will need to be created (from Data > Data inputs > TCP). See [Get data from TCP and UDP ports](http://docs.splunk.com/Documentation/Splunk/latest/Data/Monitornetworkports)

#### Generate Authorization Bearer Token for Anypoint Platform

There are 3 methods to generate an access token.

##### Method 1

|  |
| --- |
| *curl -d "username=[INSERT USER]&password=[INSERT PASSWORD]" "https://anypoint.mulesoft.com/accounts/login"* |

###### Example

$ curl -d "username=joe.blogs&password=sample.password" "https://anypoint.mulesoft.com/accounts/login"

{

**"access\_token": "d6eb5c5e-fb7e-43f7-afaf-5594a91656bc"**,

"token\_type": "bearer",

"redirectUrl": "/home/"

}

##### Method 2

|  |
| --- |
| *curl -H "Content-Type: application/json" -X POST -d '{"username":"[USERNAME]","password":"[PASSWORD]"}' https://anypoint.mulesoft.com/accounts/login*  *"* |

###### Example

$ curl -H "Content-Type: application/json" -X POST -d '{"username":"joe.blogs","password":"sample.password"}' https://anypoint.mulesoft.com/accounts/login

{

**"access\_token": "d6eb5c5e-fb7e-43f7-afaf-5594a91656bc"**,

"token\_type": "bearer",

"redirectUrl": "/home/"

}

##### Method 3

In case of external identity configured, obtain a SAML token from external identity administrator and POST to [*https://anypoint.mulesoft.com/accounts/login/receive-id*](https://anypoint.mulesoft.com/accounts/login/receive-id)API.

#### Retrieve Applications List

These are the steps to retrieve the list of applications

1. See [Generate Authorization Bearer Token for Anypoint Platform](#_Generate_Authorization_Bearer_2)
2. See [Retrieve Environment ID](#_Retrieve_Environment_ID_2)
3. Invoke **/api/v2/applications** API

|  |
| --- |
| *curl -H "Authorization: Bearer [YOUR\_ACCESS\_TOKEN]" -H "X-ANYPNT-ENV-ID: [YOUR\_ENV\_ID]" https://anypoint.mulesoft.com/cloudhub/api/v2/applications* |

curl -H "Authorization: **Bearer d6eb5c5e-fb7e-43f7-afaf-5594a91656bc**" -H "X-ANYPNT-ENV-ID: **a427405e-30ba-44a2-812b-f45c56d3c54c**" https://anypoint.mulesoft.com/cloudhub/api/v2/applications

{

    "domain": "app-new",

"fullDomain": "app-new.eu.cloudhub.io",

}

#### Retrieve Environment ID

These are the steps to retrieve Environment ID

1. See [Generate Authorization Bearer Token for Anypoint Platform](#_Generate_Authorization_Bearer_3)
2. See [Retrieve Organization ID](#_Retrieve_Organization_ID_2)
3. Invoke***/api/organizations/[YOUR\_ORG\_ID]/environments*** API

|  |
| --- |
| *curl -v -H "Authorization: Bearer [YOUR\_ACCESS\_TOKEN]" "https://anypoint.mulesoft.com/accounts/api/organizations/[YOUR\_ORG\_ID]/environments"* |

curl -H "Authorization: **Bearer d6eb5c5e-fb7e-43f7-afaf-5594a91656bc**" https://anypoint.mulesoft.com/accounts/api/ organizations/**09396371-2cd4-412e-8d08-4356dd7e7bfc**/environments

{

"id": "**a427405e-30ba-44a2-812b-f45c56d3c54c**",

"name": "Production",

}

#### Retrieve Organization ID

These are the steps to retrieve Organization ID

1. See [Generate Authorization Bearer Token for Anypoint Platform](#_Generate_Authorization_Bearer_4)
2. Invoke ***/api/me*** API

|  |
| --- |
| *curl -H "Authorization: Bearer [YOUR\_ACCESS\_TOKEN]" "https://anypoint.mulesoft.com/accounts/api/me"* |

curl -H "Authorization: **Bearer d6eb5c5e-fb7e-43f7-afaf-5594a91656bc**" https://anypoint.mulesoft.com/accounts/api/me

    "organization": {

      "name": "Mulesoft Example Organisation",

**"id": "09396371-2cd4-412e-8d08-4356dd7e7bfc"**,

      "createdAt": "2014-10-25T16:50:52.726Z",

      "updatedAt": "2016-03-04T01:16:26.715Z",

#### Retrieve Application Logs

These are the steps to retrieve application logs

1. See [Generate Authorization Bearer Token for Anypoint Platform](#_Generate_Authorization_Bearer_5)
2. See [Retrieve Organization ID](#_Retrieve_Organization_ID)
3. Invoke **/api/v2/applications/[domain]/logs** API

|  |
| --- |
| *curl –X POST -H "Authorization: Bearer [YOUR\_ACCESS\_TOKEN]" -H "X-ANYPNT-ENV-ID: [YOUR\_ENV\_ID]" –H "Content-Type: application/json" –d ‘{"lowerId":"[LAST\_FETCHED\_RECORD\_ID]"}’ "https://anypoint.mulesoft.com/cloudhub/api/v2/applications/[YOUR\_APP\_NAME]/logs"* |

curl -X POST -H "Authorization: **Bearer d6eb5c5e-fb7e-43f7-afaf-5594a91656bc**" -H "X-ANYPNT-ENV-ID: **a427405e-30ba-44a2-812b-f45c56d3c54c**" -H "Content-Type: application/json" -d '{"lowerId":**0**}' "https://anypoint.mulesoft.com/cloudhub/api/v2/applications/ **app-new**/logs"

   {

"recordId": "15DEAB0AWA6599424bae4b0a45eb3239d08-05994250B00000001",

"deploymentId": "599424bae4b0a45eb3239d01",

"instanceId": "599424bae4b0a45eb3239d01-0",

"line": 1,

"event": {

"loggerName": "org.mule.module.launcher.application.DefaultMuleApplication",

"threadName": "qtp1340000448-34",

"timestamp": 1502881032870,

"message": "\n++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++\n+ Initializing app 'app-new' +\n++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++",

"priority": "INFO",

"instanceId": ""

}

}

### Pros

* There will be no modification to the actual application(s).

### Cons

* Additional worker required to host this standalone application if built on Mule

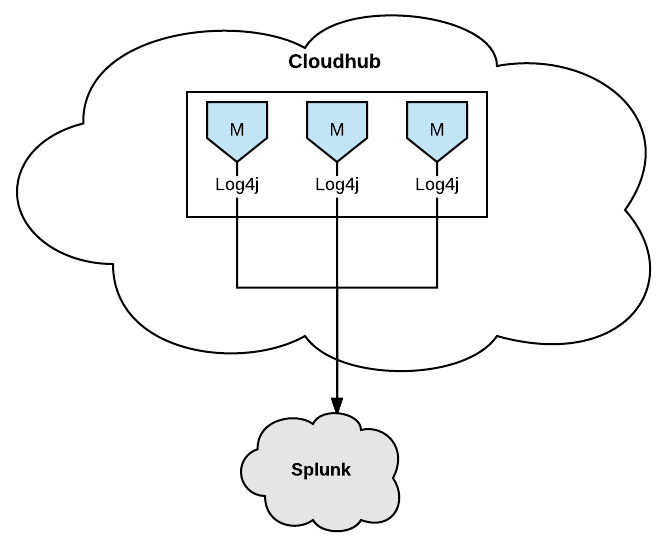
|  |
| --- |
| **We recommend this solution as it decouples the actual application from log publishing** |

### Sample project

A reference project by Mulesoft support team is available on mulesoft-consulting repository, and can be made available on request.

## Splunk Log4j Appender

This method uses the Log4j Appender to send all the events to Splunk.



### Steps

These are the steps involved in configuring the log4j appender.

|  |
| --- |
| **The internal log management would need to be disabled for this to work, and can be requested via the Support portal. See** [**https://docs.mulesoft.com/runtime-manager/custom-log-appender**](https://docs.mulesoft.com/runtime-manager/custom-log-appender) |

1. Request for “**Disable CloudHub Logs**” feature
2. Disable CloudHub logs for the application(s)
3. Follow the steps documented here: <http://dev.splunk.com/view/splunk-logging-java/SP-CAAAE3R>
4. We recommend to use the XML provided in the Runtime Manager Custom Log Appender [documentation](https://docs.mulesoft.com/runtime-manager/custom-log-appender), and then add Splunk Appender as explained in Splunk [documentation](http://dev.splunk.com/view/splunk-logging-java/SP-CAAAE3R)
5. A Splunk Enterprise TCP input will need to be created (from Data > Data inputs > TCP). See [Get data from TCP and UDP ports](http://docs.splunk.com/Documentation/Splunk/latest/Data/Monitornetworkports)

### Pros

* The log publishing will be more real time

### Cons

* Performance impact on individual applications