intake_splunk Documentation

Release 0.1.0+5.g0307223.dirty

Joseph Crail

Jul 26, 2019

CONTENTS:

This package accesses tabular data in Splunk, and can be used by Intake to load that into pandas dataframes.

CHAPTER

ONE

QUICKSTART

`intake-splunk` provides quick and easy access to tabular data stored in Apache Splunk

This plugin reads splunk query results without random access: there is only ever a single partition.

1.1 Installation

To use this plugin for intake, install with the following command:

```
conda install -c intake intake-splunk
```

1.2 Usage

1.2.1 Ad-hoc

After installation, the function `intake.open_splunk` will become available. It can be used to execute queries on the splunk server, and download the results as a list of dictionaries.

Three parameters are of interest when defining a data source:

- query: the query to execute, using Splunk's **'Query Syntax'_**

1.2.2 Creating Catalog Entries

To use, catalog entries must specify `driver: splunk`.

1.2.3 Using a Catalog

CHAPTER

TWO

API REFERENCE

intake_splunk.core.SplunkSource(query, url, auth)	Execute a query on Splunk

class intake_splunk.core.**SplunkSource**(*query*, *url*, *auth*, *chunksize=5000*, *metadata=None*)

Execute a query on Splunk

Parameters

query [str] String to pass to Splunk for execution. If it does not start with "|" or "search", "search" will be prepended.

url [str] Endpoint on which to reach splunk, including protocol and port.

auth [(str, str) or str] Username/password to authenticate by.

chunksize [int]

Attributes

cache_dirs

classname

datashape

description

has_been_persisted

hvplot Returns a hvPlot object to provide a high-level plotting API.

is_persisted

plot Returns a hvPlot object to provide a high-level plotting API.

plots List custom associated quick-plots

Methods

close(self)	Close open resources corresponding to this data source.
discover(self)	Open resource and populate the source attributes.
export(self, path, **kwargs)	Save this data for sharing with other people
persist(self[, ttl])	Save data from this source to local persistent storage
read(self)	Load entire dataset into a container and return it

Continued on next page

Table 2 – continued from previous page

read_chunked(self)	Return iterator over container fragments of data source
read_partition(self, i)	Return a part of the data corresponding to i-th partition.
to_dask(self)	Return a dask container for this data source
to_spark(self)	Provide an equivalent data object in Apache Spark
yaml(self[, with_plugin])	Return YAML representation of this data-source

get_persisted	
set_cache_dir	

to_dask(*self*)

Return a dask container for this data source

CHAPTER

THREE

INDICES AND TABLES

- genindex
- modindex
- search

INDEX

S

T