**Canvas Technology Add-On for Splunk (v 1.0.3)**

## OVERVIEW

The Canvas Technology Add-On (TA) for Splunk collects information from Instructure's Canvas LMS – REST API ( https://canvas.instructure.com/doc/api/ ).

In this release, the following information is collected from Canvas:

- Authentication Logs (sourcetype = canvas:authentication)

## MERGE CONTEXTUAL INFORMATION

When you collect the authentication logs, you need to decide if you want to include any of the user, login, account, or page view contextual information in the raw event (i.e. name, username, login_id, …). This is configured in the SETUP THE REQUIRED PARAMETERS (CANVAS.CONF) section below.

Without this info, there will only be an ID (or null for page views) without any actual link to the referenced information. For example, if you just request the authentication data without context, you get something like the following:


```
{ [-]
  created_at: 2016-04-28T16:42:40Z
  event_type: login
  id: a3804d13-8fc0-4a16-9f41-56d3cb24f211
  links: { [-]
      account: 1
      login: 2
      page_view: null
      user: 2
  }
}
```


Notice the links section has ID's for account, login, page_view, and user. If you want to enrich the linked ID's with actual values, that is when you would add any of the other sections. For example, the following shows the add-on having enabled login and user info (which is the default).


```
{ [-]
  created_at: 2016-04-28T16:42:40Z
  event_type: login
  id: a3804d13-8fc0-4a16-9f41-56d3cb24f211
  links: { [-]
    account: 1
    login: 2
    page_view: null
    user: 2
  }
```

```
  login: { [-]
    account_id: 1
    authentication_provider_id: null
    id: 2
    integration_id: null
    sis_user_id: null
    unique_id: mgildenhorn@splunk.com
    user_id: 2
  }
  user: { [-]
    id: 2
    login_id: mgildenhorn@splunk.com
    name: Matt Gildenhorn
    short_name: Matt Gildenhorn
    sortable_name: Gildenhorn, Matt
  }
}
```


**GATHER REQUIRED INFORMATION**

The following information needs to be collected before the TA can be enabled:

- Canvas server name (i.e. yoursite.instructure.com)
- Root Account ID – At the root level of your Canvas LMS hierarchy, your administrator(s) belong to this account ID (i.e. 1). Default is 1.
- Canvas Access Token – Unique access token tied to a root hierarchy administrator's account profile in Canvas. All calls to the API are made using this token, which requires the user who owns the token to be a root hierarchy administrator account in Canvas. This is to ensure that the account will have full read privileges.
- Number of events per page – Used to control how many events come back at once. This is to reduce the overhead on the Splunk server. All events for a given time range will be returned in a single run, however they will be split into pages of the size defined here. Default page size is 1000.
- Initial Run - Start Date/Time for collecting events – For the FIRST RUN ONLY, the start date/time you want to begin collecting events from.
- Initial Run - End Date/Time for collecting events – For the FIRST RUN ONLY, the end date/time you want to finish collecting events at. Events are collected up to but NOT including this end date/time.

**How to obtain the Root Account ID**

- You must be logged into Canvas as a root hierarchy administrator
- Go to your Canvas site accounts page: i.e. yoursite.instructure.com/accounts
- Click into your main account
- Look at the URL for the number at the end: i.e. yoursite.instructure.com/accounts/1
- The number at the end is the root account ID

**How to obtain the Access Token**

- You must be logged into Canvas as a root hierarchy administrator (Note: This account must have total read access to the Canvas system)
- Go to your Canvas site profile page: i.e. yoursite.instructure.com/profile
- Scroll down to the 'Approved Integrations:' section
- Click on the 'New Access Token' button:
    - Enter a purpose: i.e. 'Splunk-Canvas Integration'
    - Leave expiration date blank if you want it to stay indefinitely
    - Click the 'Generate Token' button
- Write the token down because it will NOT be shown again on the screen, nor can you pull it up again if you lose the token.

**INSTALL THE ADD-ON ON ALL THE PROPER SPLUNK TIERS**

The Canvas TA gets installed on a Heavy Forwarder. Universal Forwarders cannot be used because python is required. Additional setup information for each tier is listed here:

- Indexers – The Canvas TA wants to send the data to an index called 'canvas' by default in the setup. If you choose to use that index, you will need to create that index on each of your indexers BEFORE you enable the input. Otherwise, please change/define the name of the correct index in the auth_logs input during the setup. There is an example indexes.conf in the README/ directory which defines an index called 'canvas' if you wish to use it on your Indexers.
- Heavy Forwarder – This is the machine that makes the connection to the Canvas API, so please make sure connectivity exists to it and also to the Indexers.
    - This is the machine where all of the setup/configuration needs to occur. Set up instructions are listed below.

**On the heavy forwarder, there are 2 primary steps to set up the TA (Described in detail below):**

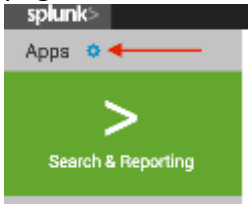
1. **SET UP THE REQUIRED PARAMETERS (via GUI or by editing CANVAS.CONF)**
2. **SET UP THE INPUTS (via GUI or by editing INPUTS.CONF)**

## 1. SET UP THE REQUIRED PARAMETERS (via GUI or by editing CANVAS.CONF)

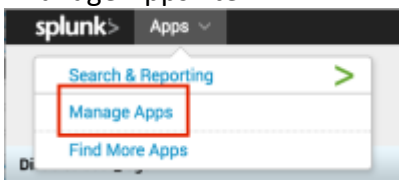
### Set Up the Required Parameters (In the GUI):

Once the required information (listed above) has been gathered, enter it into the TA. This should be done on the heavy forwarder, and optionally the search head if the user lookup is to be enabled. No work needs to be done on the Indexers.

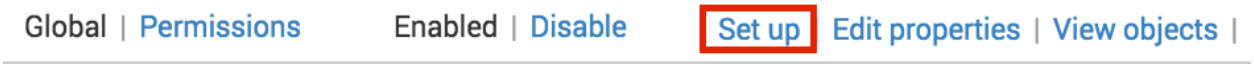
- Go to the 'Manage Apps' page.
  - In the newer versions of Splunk, you can get there by going to the main Splunk page, and then selecting the 'Manage Apps' gear in the upper left.




  - In the older versions of Splunk (as well as the newer), you can click the 'Apps' dropdown from the very top left next to the Splunk logo, and then select the 'Manage Apps' item.




- Find the App named 'Canvas Add-On For Splunk', and then click on the 'Set up' in the Actions section on the right




- Fill in ALL of the parameters with the information collected above. Click 'Save' at the bottom right when complete.
  - **Shared Parameters** - These parameters are used commonly across all Canvas API calls.
    - Canvas Server Name
    - Canvas Root Account ID (Default 1)
    - Canvas Access Token

        - Events Per Page - Number of events that gets returned at a time. Used to control the size/memory used for the amount of data returned. In a single run, the add-on will continue grabbing events of this size, until all events have been returned. (Default 1000)
    - **Initialization Parameters** - These parameters are used during the **FIRST RUN ONLY**. After initial run, the app keeps track of future entries called in separate config files.
        - Start Date/Time (First Collection Only)
        - End Date/Time (First Collection Only)
    - **Authentication Log Specific Parameters** – These parameters are used for the 'auth_logs' input. They merge the contextual information for user, login, account, and page view into each event. Without this info, there will only be an ID (or null for page views) without any actual link to the referenced information.
        - Merge User Info (Default is checked = Enable)
        - Merge Login Info (Default is checked = Enable)
        - Merge Account Info (Default is unchecked = Disable)
        - Merge Page View Info (Default is unchecked = Disable)

**Set Up the Required Parameters (via the Command Line):**

- Ensure that the canvas_ta was installed under $SPLUNK_HOME/etc/apps
- Go to the canvas_ta directory under $SPLUNK_HOME/etc/apps
- Copy the canvas.conf from the canvas_ta/default directory to the canvas_ta/local directory
- Enter the required information into the canvas.conf file in the following locations/parameters (see above in the GUI section for descriptions of all the parameters):
    - Canvas Server Name – **canvasurl**
    - Root Account ID – **rootaccountid** (Default 1)
    - Canvas Access Token – **canvastoken**
    - Number of Events Per Page – **per_page** (Default 1000)
    - Initial Run - Start Date/Time – **start_time**
    - Initial Run - End Date/Time – **end_time**
    - Merge User Info – **merge_users** [0|1] (Default 1 = Enable)
    - Merge Login Info – **merge_logins** [0|1] (Default 1 = Enable)
    - Merge Account Info – **merge_accts** [0|1] (Default 0 = Disable)
    - Merge Page View Info – **merge_pageviews** [0|1] (Default 0 = Disable)

## 2. SET UP THE INPUTS (via GUI or by editing INPUTS.CONF)

You can either set up the input using the GUI or Command Line:

- Set up 'auth_logs' Input in the GUI
    - Go to 'Settings -> Data Inputs -> Canvas', click on the 'auth_logs' Canvas Input Name

    - Change settings as needed and click 'Save' when done.
        - Polling Interval can be either in CRON format or in Seconds format.
            - Default is 600 seconds (or 10 minutes).
        - Set a host name for the input, such as the Canvas hosted sitename (i.e. your.instructure.com)
        - The default index is named 'canvas', which you can edit as needed. *Please remember to create the 'canvas' index (or whatever you wish to call it) on all your Indexers before you enable the input.*
    - When ready to start the input, click 'Enable'
- Set up 'auth_logs' Input via the command line:
    - Copy the 'auth_logs' inputs.conf settings from the <canvas_ta>/default directory to the <canvas_ta>/local directory and edit it
    - Change the parameters as necessary
        - Enable the Input
            - Set disabled = 0 to "enable" the input
        - Polling Interval (polling_interval) can be either CRON format or in Seconds format. Default is 600 seconds (or 10 minutes).
        - Set a host name for the input (host = …), such as the Canvas hosted sitename (i.e. YOURSITE.instructure.com)
        - The default index is named 'canvas' (index = canvas), which you can edit as needed. *Please remember to create the 'canvas' index (or whatever you wish to call it) on all your Indexers before you enable the input.*
    - Restart Splunk instance

**CONTACT**

Matt Gildenhorn
mgildenhorn@splunk.com

**ACKNOWLEDGEMENT**

Current version of the Canvas TA came from a heavily modified version of the REST API Modular Input by Damien Dallimore (https://splunkbase.splunk.com/app/1546/)

**FINALLY, A BIG THANK YOU** to Scott Robards and Nick Young for helping test and tweak along the way.

**VERSIONS**

1.0.1 – Initial release
1.0.2 – Simplified the inputs section. Removed the default indexes definition for the Indexers due to Splunk best practices. Modified the add-on to be compliant with Splunk Certification.
1.0.3 – Fixed issue when calling SSL URL Request library in responsehandlers, where in certain cases, SSL call was looking for a pem directory that does not exist. Disabled the verification to fix it.