Splunk integration with Blue Prism® v6

Introduction

Splunk is a data collection and analysis tool which can be used to consume data Blue Prism records as part of its normal operations and diagnostics output.

Although Splunk is a generic data capture and reporting tool that can be used to analyse a variety of data, Blue Prism Version 6 has been specifically programmed an interface for Splunk such that it can be configured to consume Blue Prism's session log data.

This document provides a walkthrough of the steps required to configure Splunk to consume Blue Prism's session log information for reporting purposes.

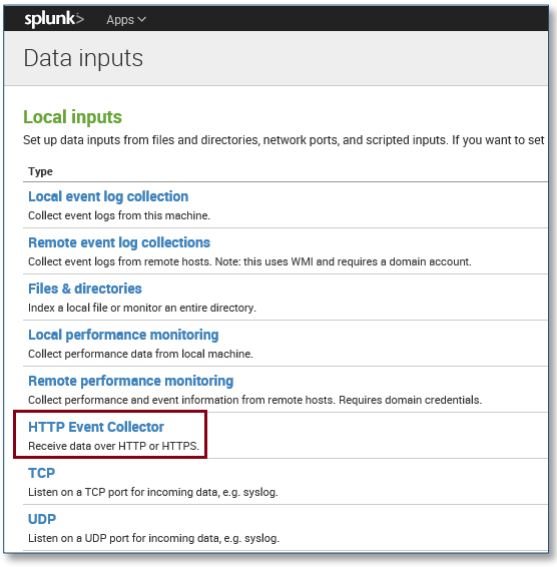
Quick Start

To get the Splunk software set up, please follow the Walkthrough available here:

http://www.splunk.com/en_us/download.html

Configuring Splunk

Log into Splunk and configure the following settings to enable data capture for Blue Prism session log data.

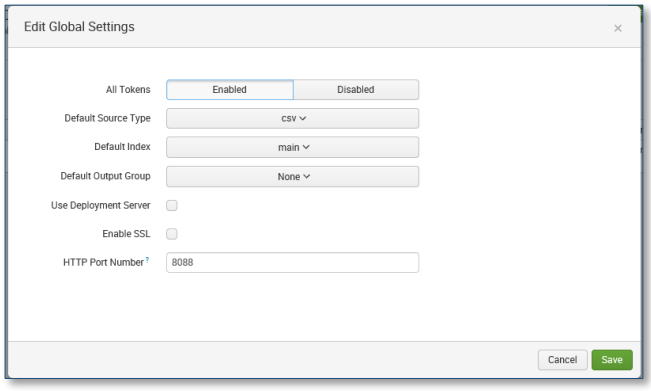


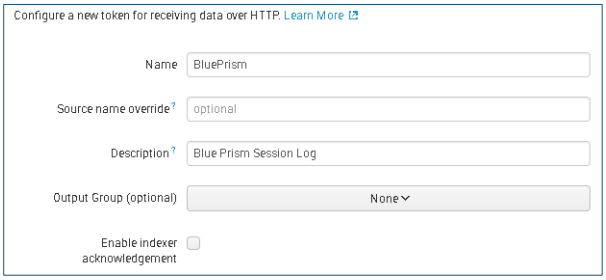
Navigate to the HTTP Event Collector

- To do this, go to Settings > Data Inputs.
- Now in the list click on HTTP Event Collect
- In the top right corner click on Global Settings

Enable HTTP Data Collection (HEC)

- Edit **Global Settings** to enable all tokens, set the SSL setting and the HTTP listening port number which Splunk will use to gather data as follows.
- Save the changes.

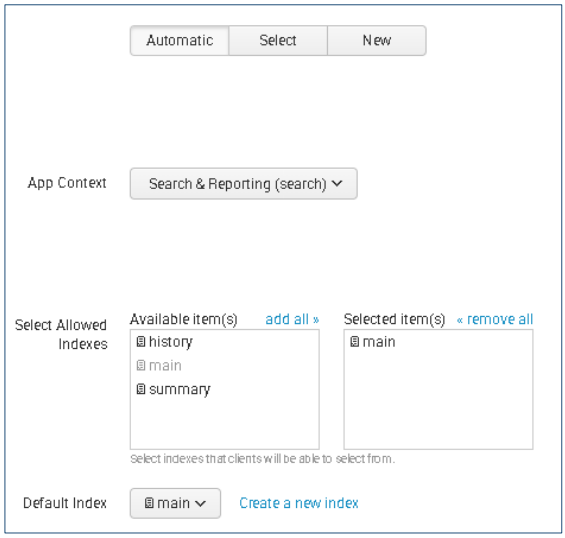


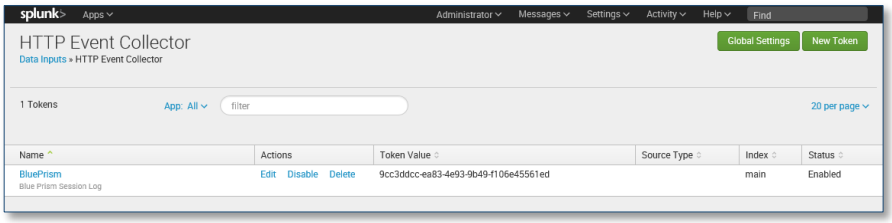


Create a new Token

- Edit **Global Settings** to enable all tokens, set the SSL setting and the HTTP listening port number which Splunk will use to gather data as follows.
- Click New Token located top right
- This token has been configured to examine the status of a Blue Prism Session Log. Choose **New Token** to go to the **Add Data** screen, or use the **Add Data → Monitor** option from the home page.

- Then click Next > at the top
- Complete the form as shown here





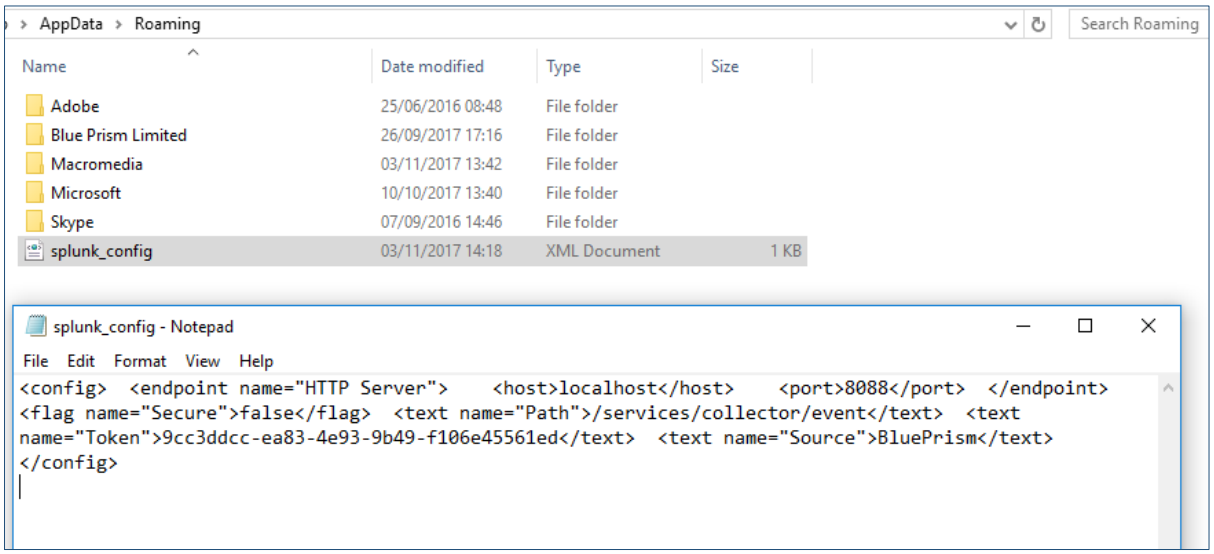
Generate a Token Value identifier string

- Record the Token Value string for use in the Blue Prism configuration file later in the process.

Configuring Blue Prism

The requirements for Blue Prism are:

- Version 6.0
- A configuration file called “splunk_config.xml” in the %appdata% directory (e.g. C:\Users\<user>\AppData\Roaming)



Configuration file

The “splunk_config.xml” configuration file is an XML file which has the following parameters in this format:

splunk_config.xml configuration file

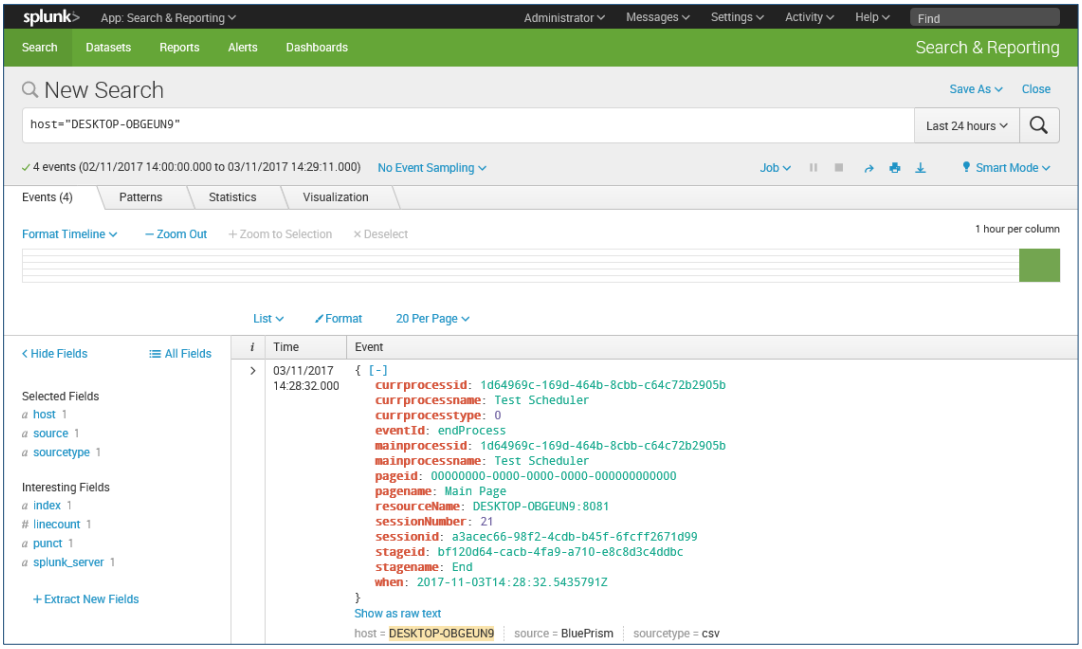
```
<config>
<endpoint name="HTTP Server">
<host>localhost</host>
<port>8088</port>
</endpoint>
<flag name="Secure">false</flag>
<text
name="Path">/services/collector/event</text
>
<text name="Token">9cc3ddcc-ea83-4e93-9b49-
f106e45561ed</text>
<text name="Source">BluePrism</text>
</config>
```

File Parameter Definitions

- <host> : the machine where the data is being retrieved from (e.g. the machine hosting the Session Log data). This is usually the machine where the Blue Prism database resides.
- <port> : the port number on the <host> machine. This is configured in Splunk and used to obtain the Blue Prism data.
- <Secure> : the Enable SSL parameter in the Global Settings of Splunk.
- <Token> : the Token Value of the HTTP Event Collector.
- <Source> : the HTTP Event Collector Name

Turn off the server service and restart the server service for the service to find and pick up the xml file.

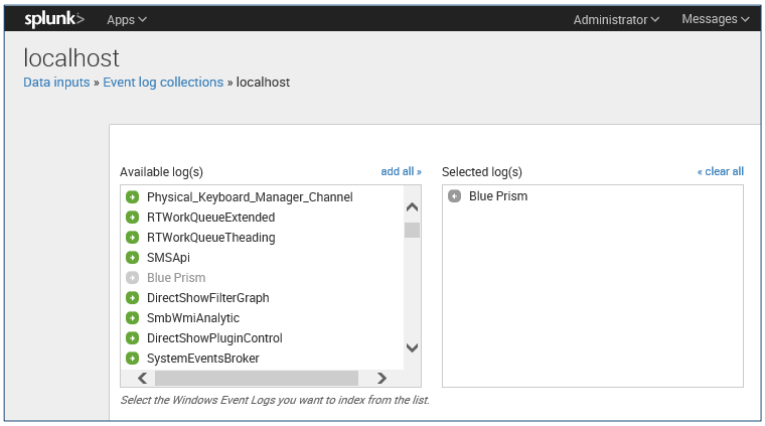
Here's an example of a report from Blue Prism's Session Log data which can be obtained from the **Search and Reporting** section in Splunk:



Event Log data

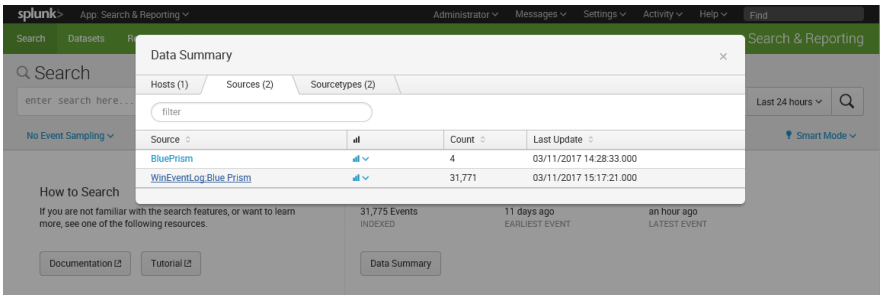
If required, it is possible to add the Blue Prism Event Log for the monitoring of events logged by Blue Prism activities.

Configuring Splunk for Event Log analysis



- Record the Token Value string for use in the Blue Prism configuration file later in the process.
- Add a new **Data Input**
- Select the Local Event Log Collection data input
- Browse to the **Blue Prism** event log

- **Save** the configuration
- In the Search and Reporting section choose the WinEventLog:Blue Prism source



Here's an example of a report from Blue Prism's Event Log data: