2015

Tanium: Splunk Application

TANIUM INC. | 1625 Shattuck Avenue, Suite 200 | Berkeley, California | 94709-1668

Contents

Tanium Splunk Application

Introduction

Tanium is a new approach to endpoint management and security monitoring that delivers instant visibility and responsiveness that does not slow down as the enterprise environment scales.

The Tanium Connect is designed to provide a broad range of integration options to extend the endpoint data collected by the Tanium server to your existing eco-system of Enterprise Security, Systems Management, and Asset Management Platforms. The Tanium Connect provides out-of-the-box integration with Splunk.

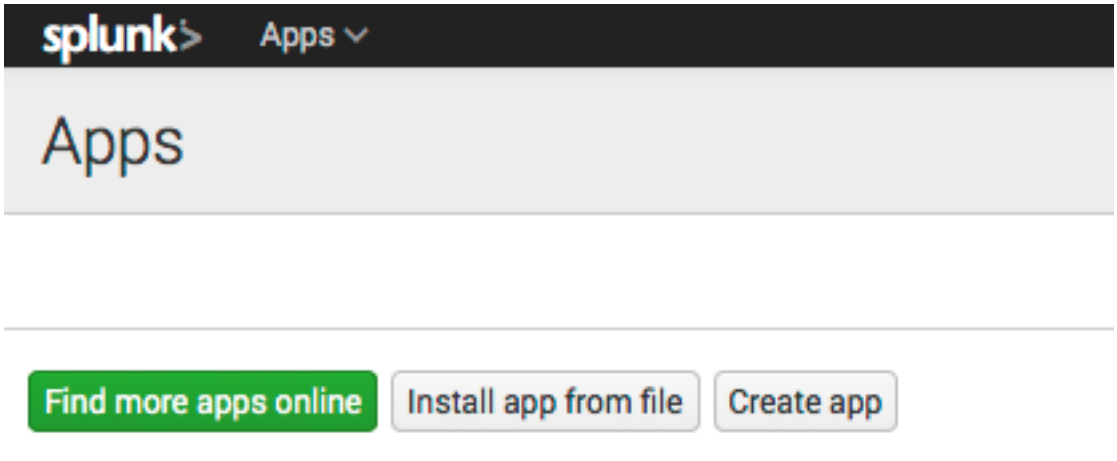
The Tanium Splunk Application contains a set of dashboards that correspond to a fixed set of questions that populate the data. The dashboards display critical software vulnerabilities, unmanaged assets, application and process visibility, detailed asset management information, suspicious open ports and external connections, web browser history, network information, and VirusTotal results.

Installation

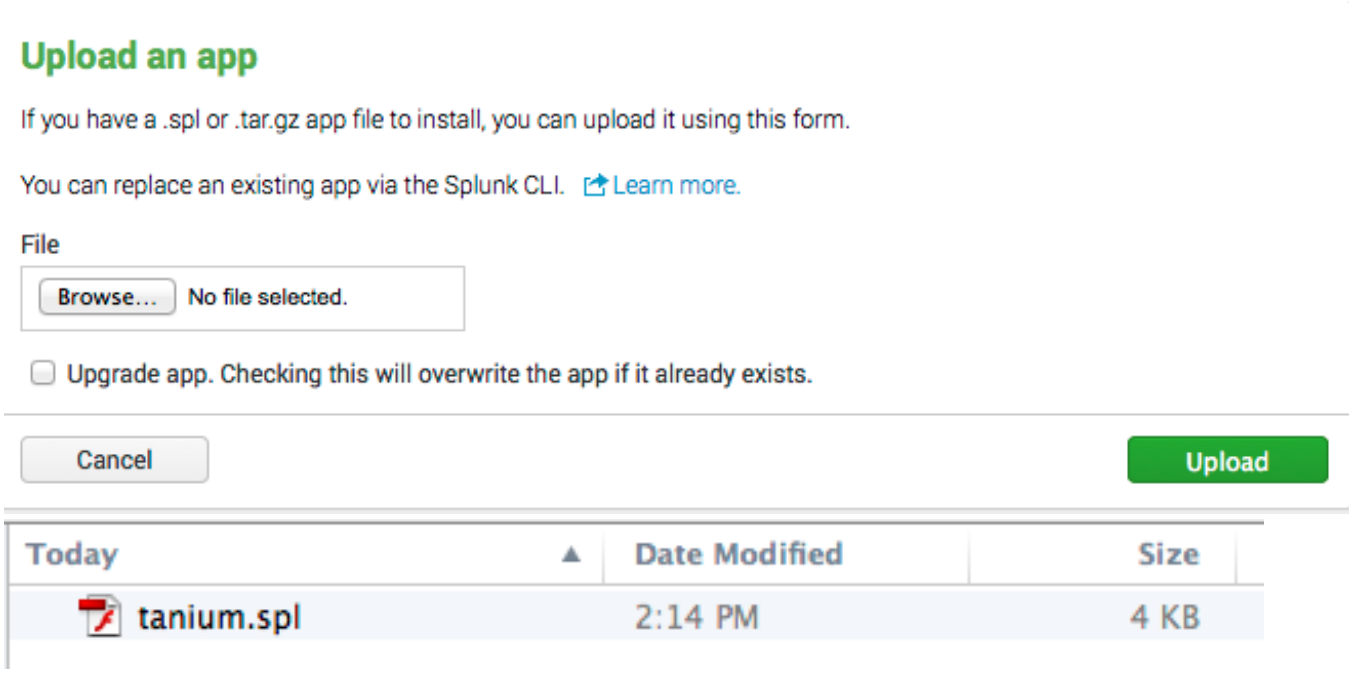
The Tanium Splunk application is developed in coordination with a fixed set of saved questions to feed the various Tanium Splunk dashboards. Therefore, there are three steps to installing the Tanium Splunk application. Step one is to install the Tanium Splunk Application into Splunk and configure a data input with sourcetype=tanium. The second step is to install the Splunk saved questions using the Tanium Console. Finally, you need to configure the Tanium Connect.

Installing the Tanium Splunk Application

1. Download the Tanium Splunk Application from http://apps.splunk.com/app/1862/
2. To install the Tanium Splunk application, first login to your Splunk environment.
3. From the Home screen, click on Manage Apps.



4. Click Install app from file.

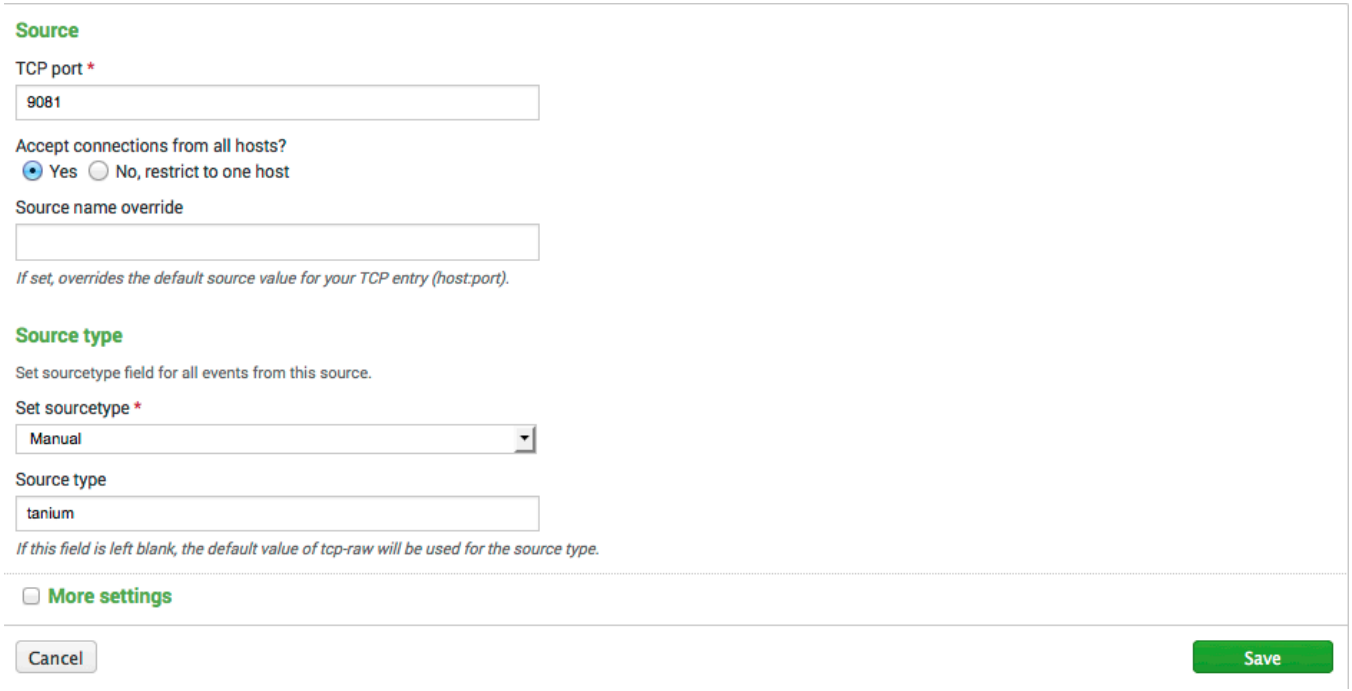


5. Click Browse. Navigate to the location of the Tanium Splunk Application, select it and click Upload.

Once the Tanium Splunk Application is successfully installed, you should see the Tanium Splunk Application on your Home screen.

Adding a Data Input for Tanium

1. From Settings, select Data Inputs. In this example, we are adding and configuring a TCP port for incoming data. Select TCP, and then select New.

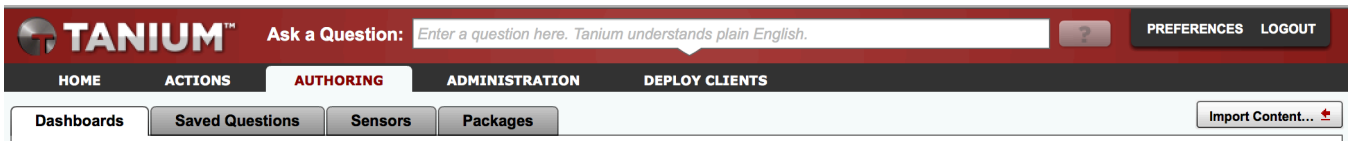


2. Enter the TCP Port you would like to listen on for incoming data. Make sure this port does not conflict with any other applications in your environment.
3. Set sourcetype to Manual
4. Enter tanium for Source type.
5. Click Save.

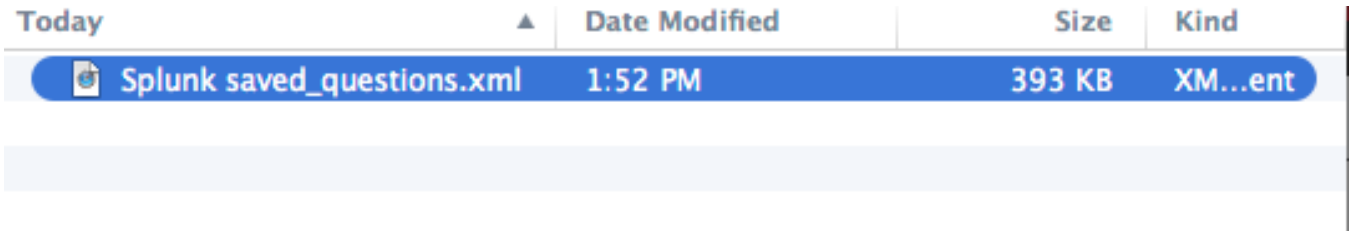
Importing Splunk Application Saved Questions thru the Tanium Console

To install the Splunk Saved questions, login to the Tanium Console.

1. Select Authoring.



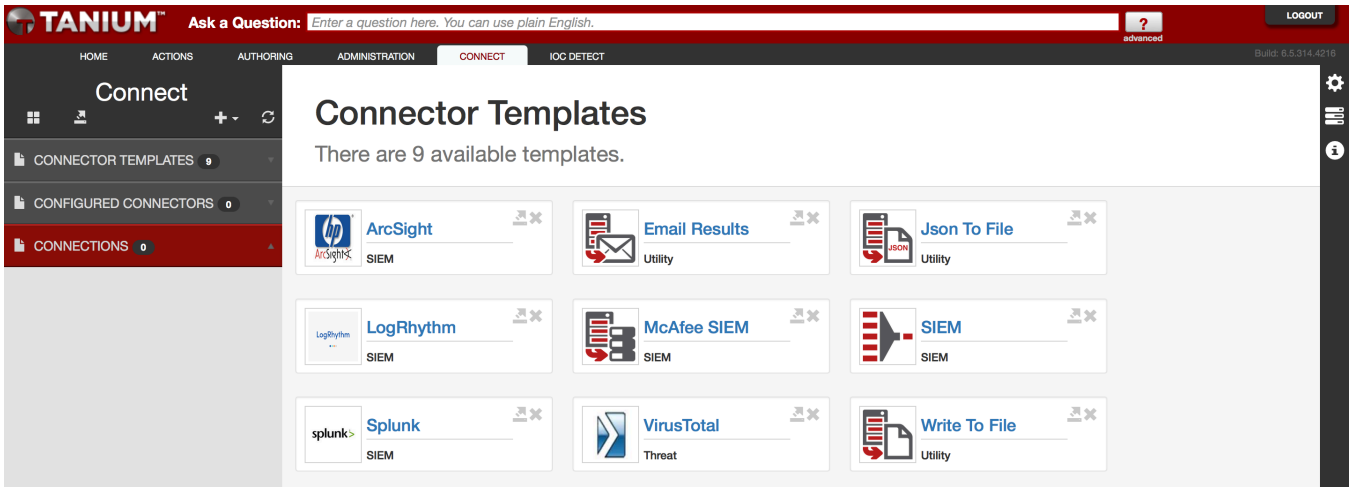
2. Select Import Content.
3. Navigate to the Splunk saved_questions.xml and select it



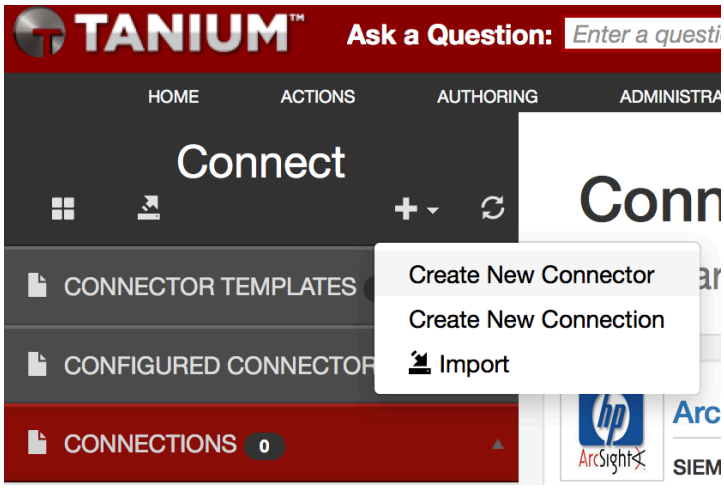
Select Replace Duplicate in database if prompted.

Configuring Splunk Connector in Tanium Connect

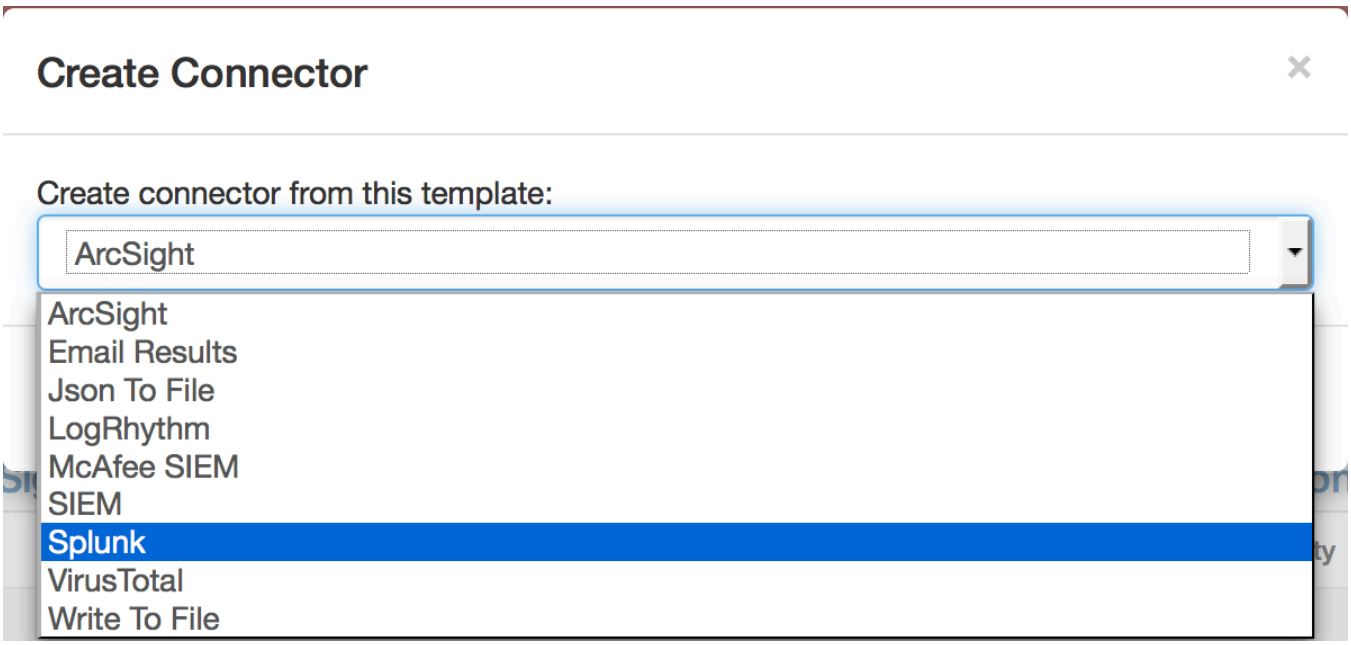
It is assumed you have properly configured the Tanium Connect plug-in to communicate with the Tanium Server.



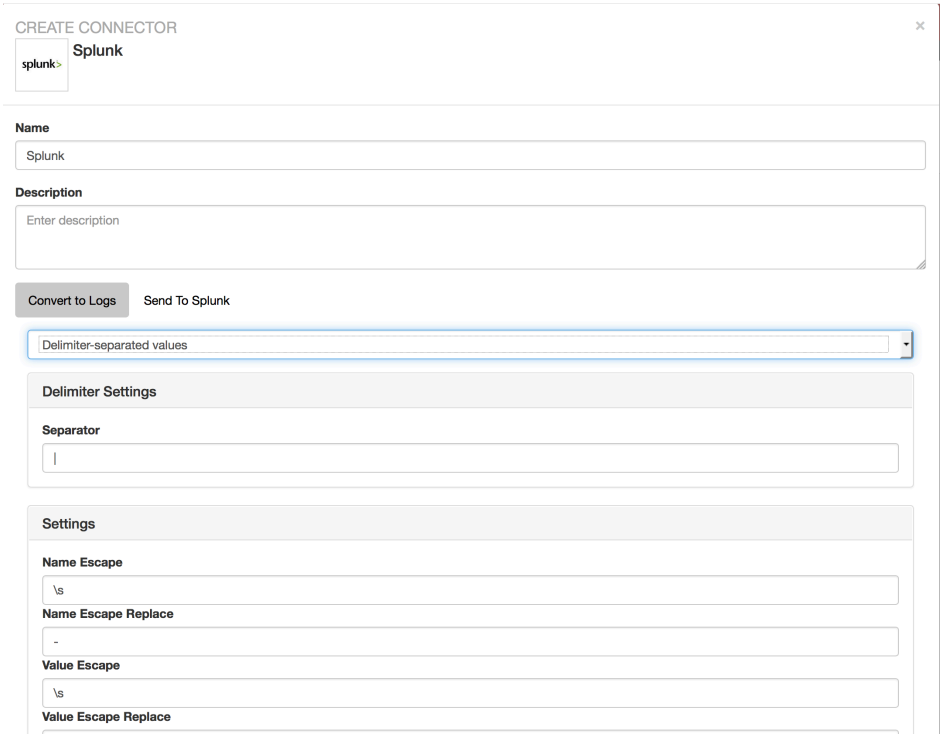
1. From the Connect left pane, click on the "+" and select Create New Connector.



2. Expand the Create Connector frøm this template, scroll down and select Splunk

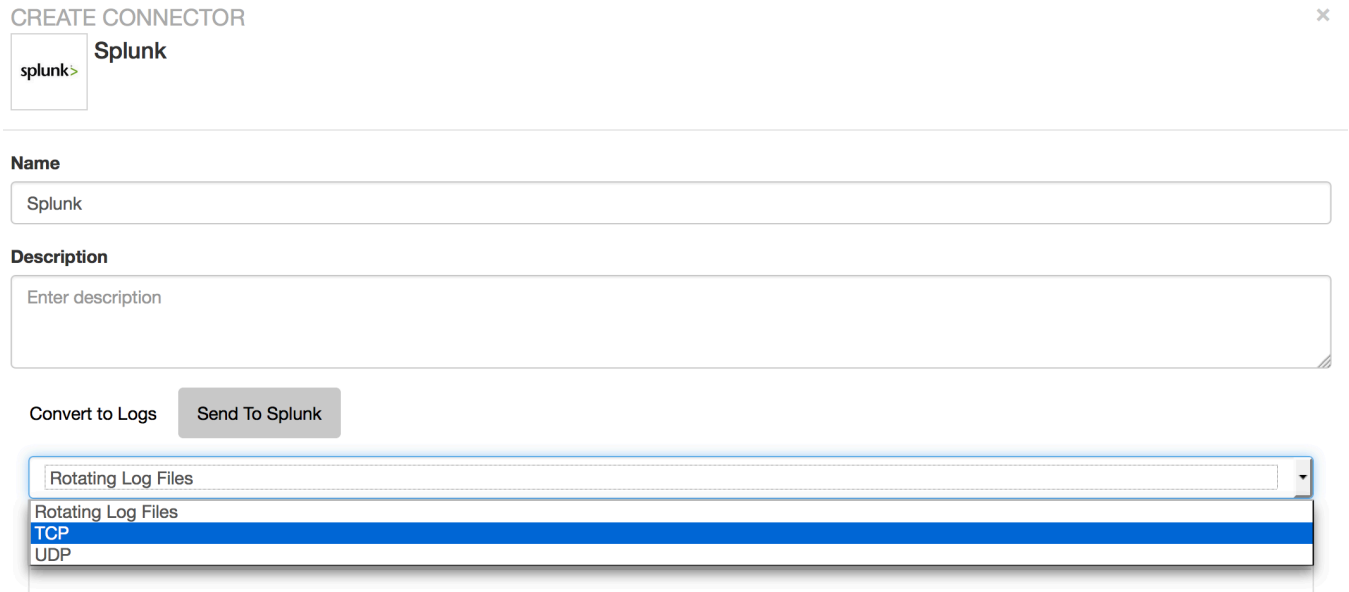


3. Click Next.

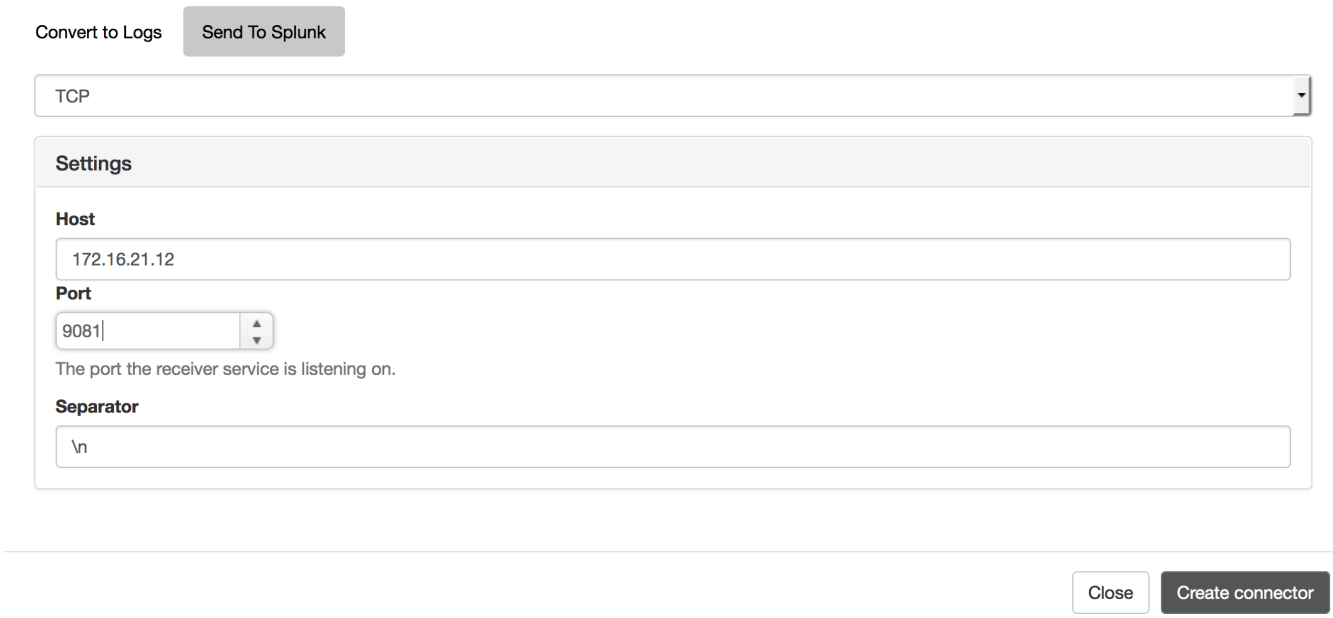


4. Click on the Convert to Logs button.

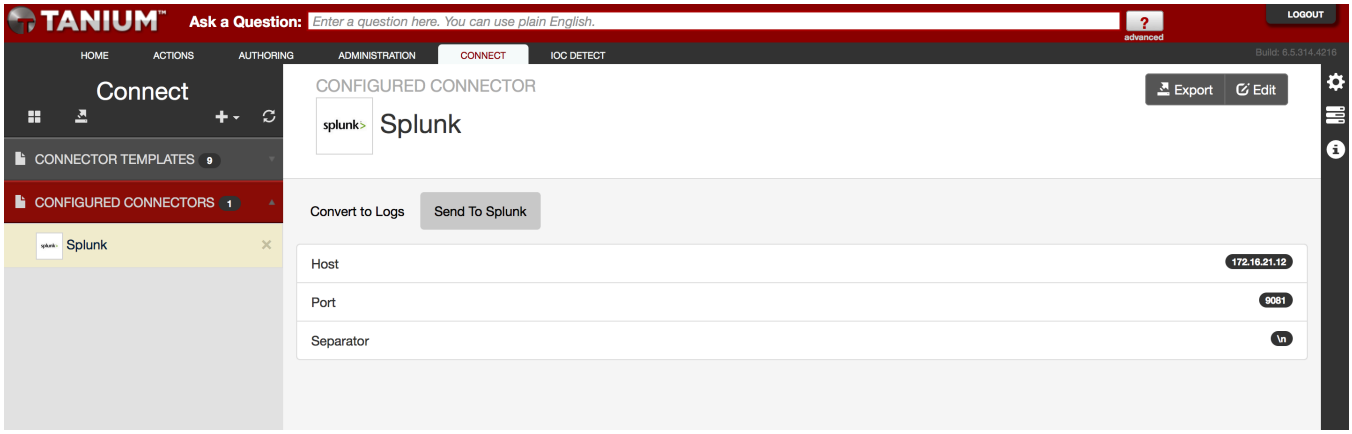
5. Select Syslog (RFC5424) from the drop-down list
6. Click on the Send To Splunk button.



7. Select TCP Receiver from the drop-down list



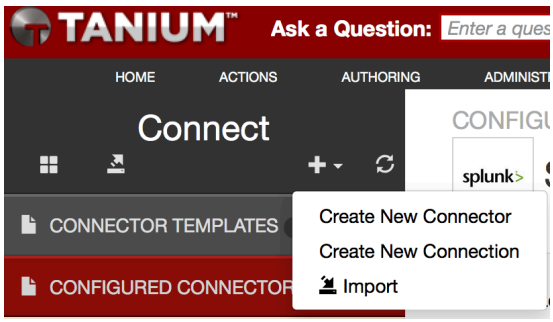
8. Enter the Splunk Server Hostname or IP address and the TCP port you defined as the Data Input for sourcetype tanium.
9. Click Create connector
   You will now see the Splunk Connector in the Configured Connectors Pane



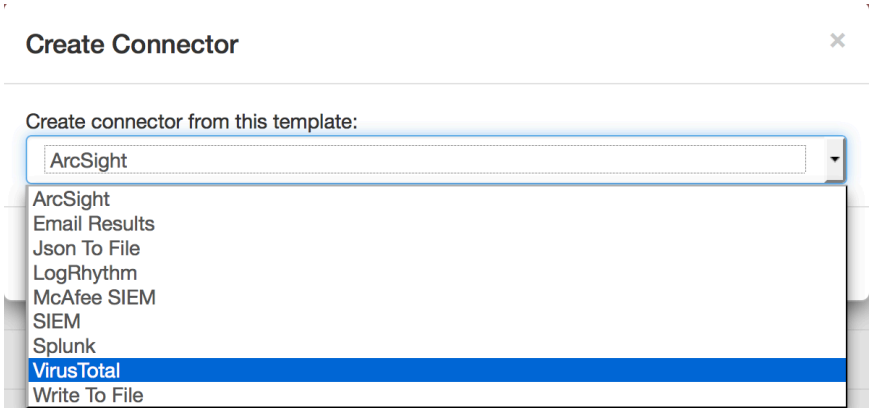
Configuring VirusTotal Connector in Tanium Connect

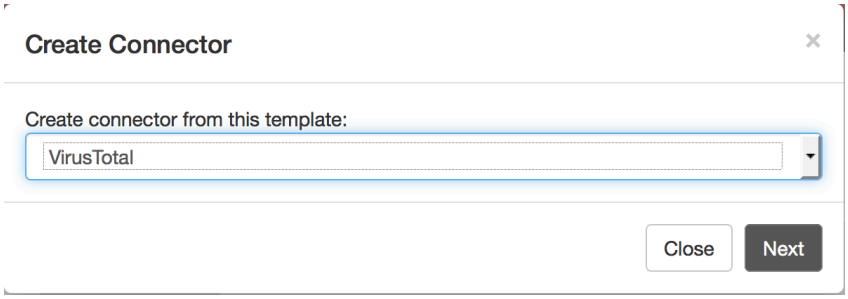
In addition to the Splunk Connector, you also need to configure the VirusTotal Connector.

1. From the Connect pane, click on the "+" and select Create New Connector.

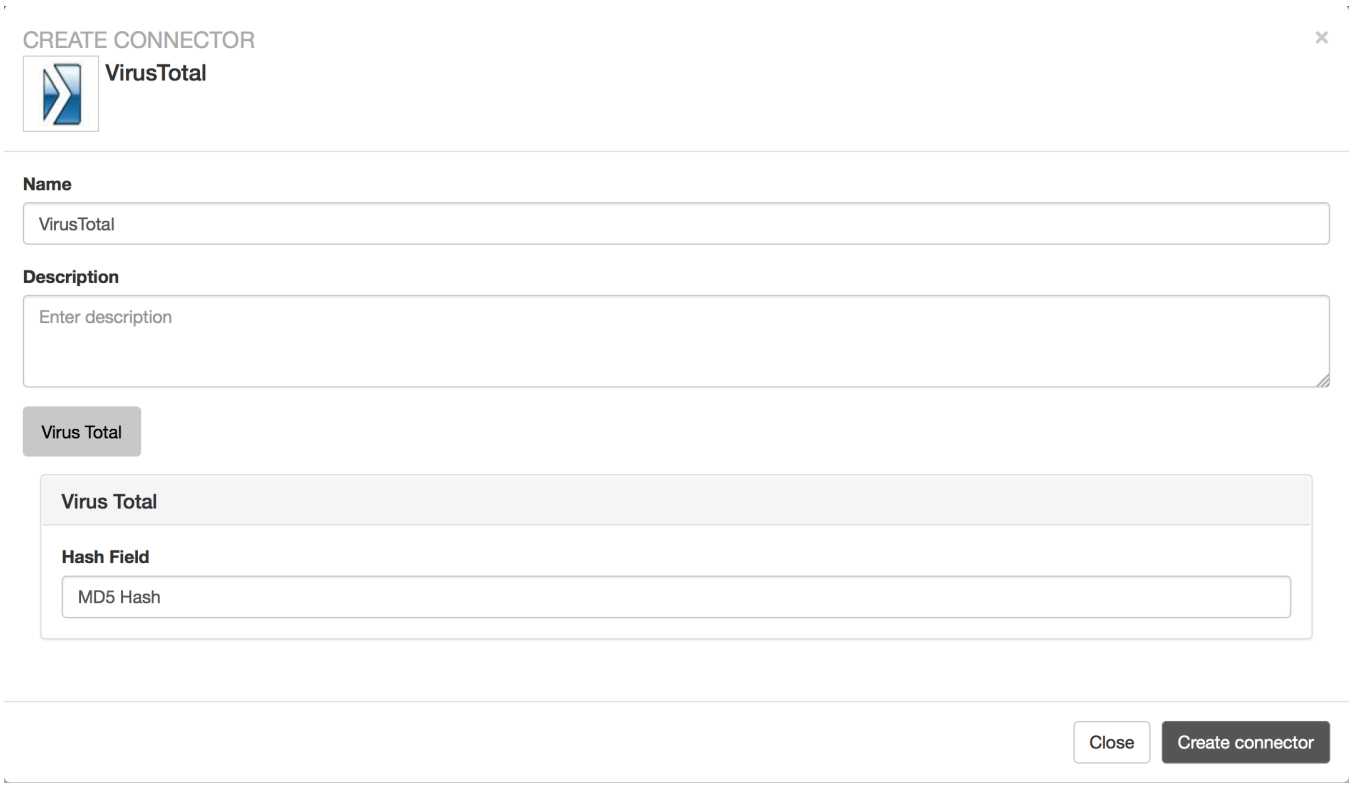


2. Scroll down and select VirusTotal

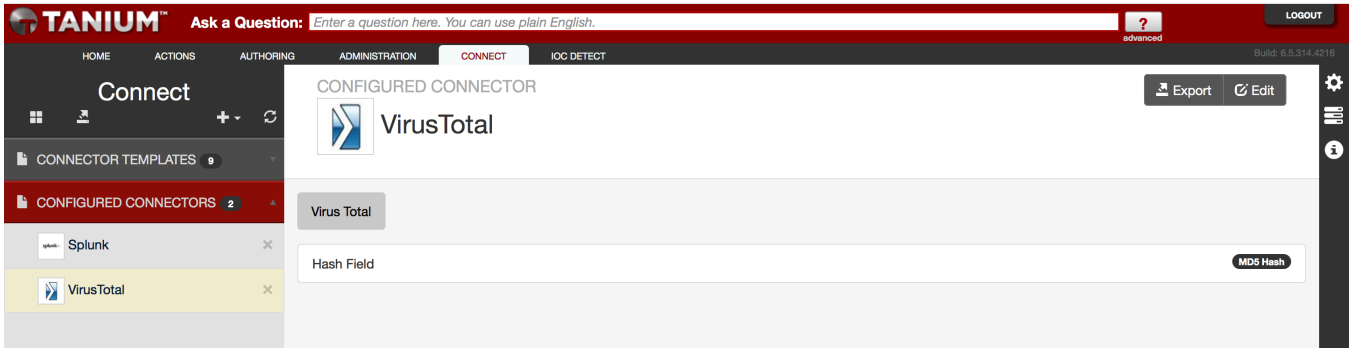




3. Click Next.



4. Click Create Connector



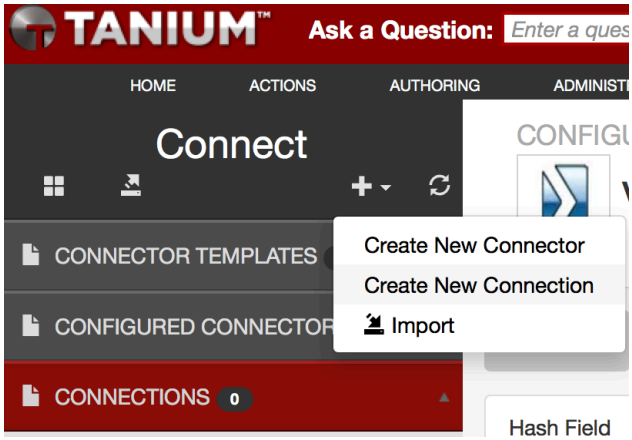
You have now successfully configured the VirusTotal Connector.

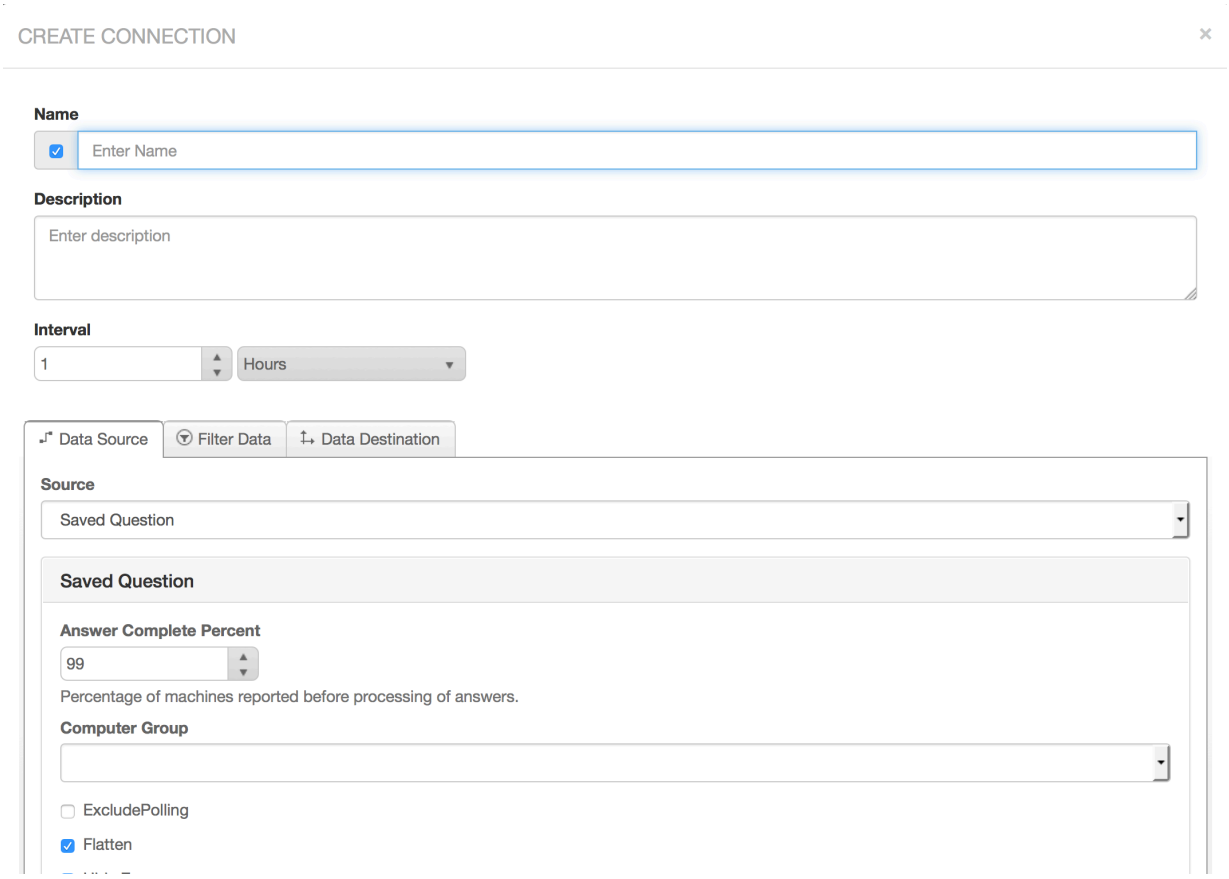
Adding Splunk Saved Questions in Tanium Connect

Once you have configured the Splunk Connector and the VirusTotal Connector in Tanium Connect, you must now configure the saved questions that feed the Tanium Splunk Application dashboards.

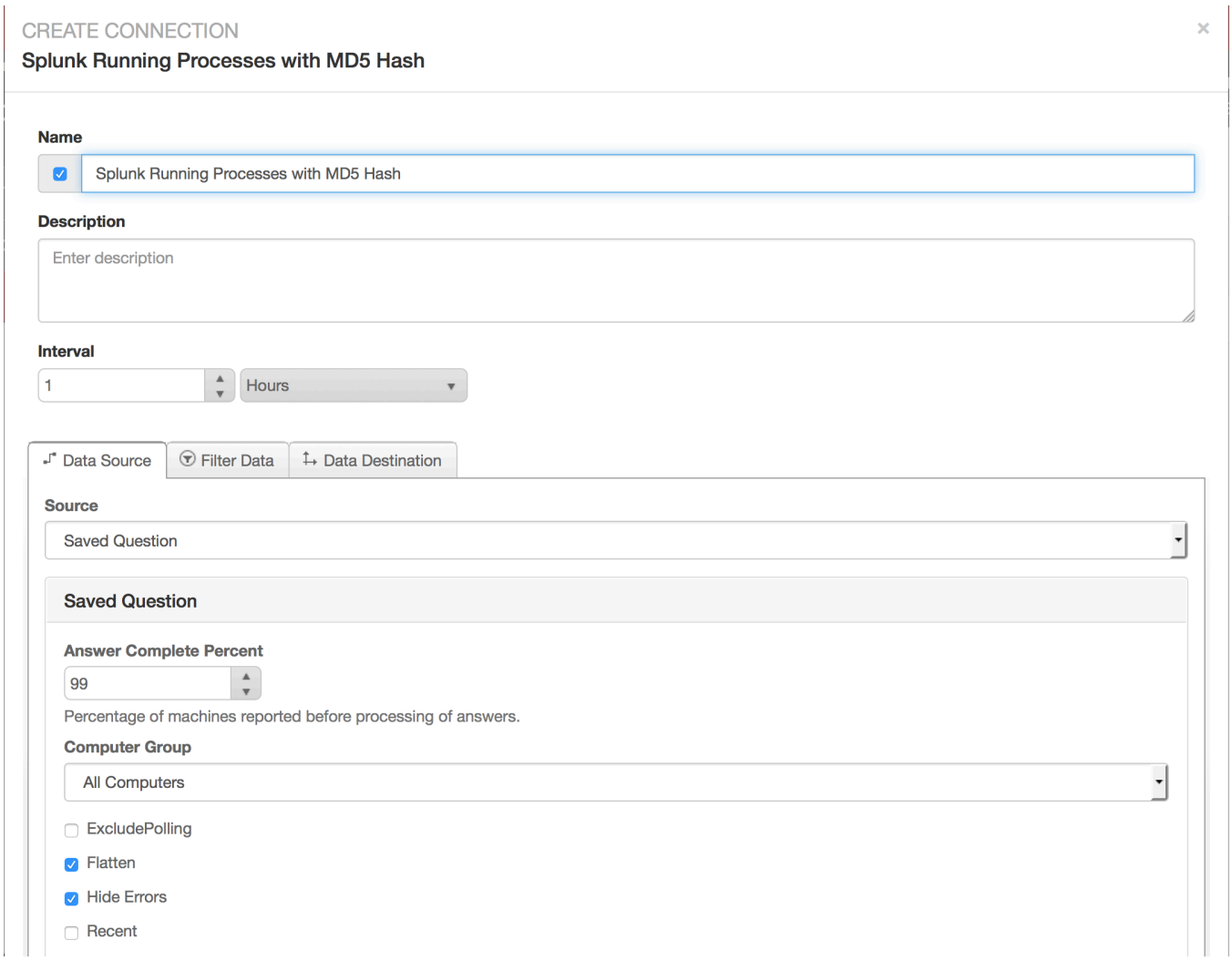
Adding Splunk Running Processes with MD5 Hash question for VirusTotal Connector

1. From the Connect pane, click on the "+" and select Create New Connection.

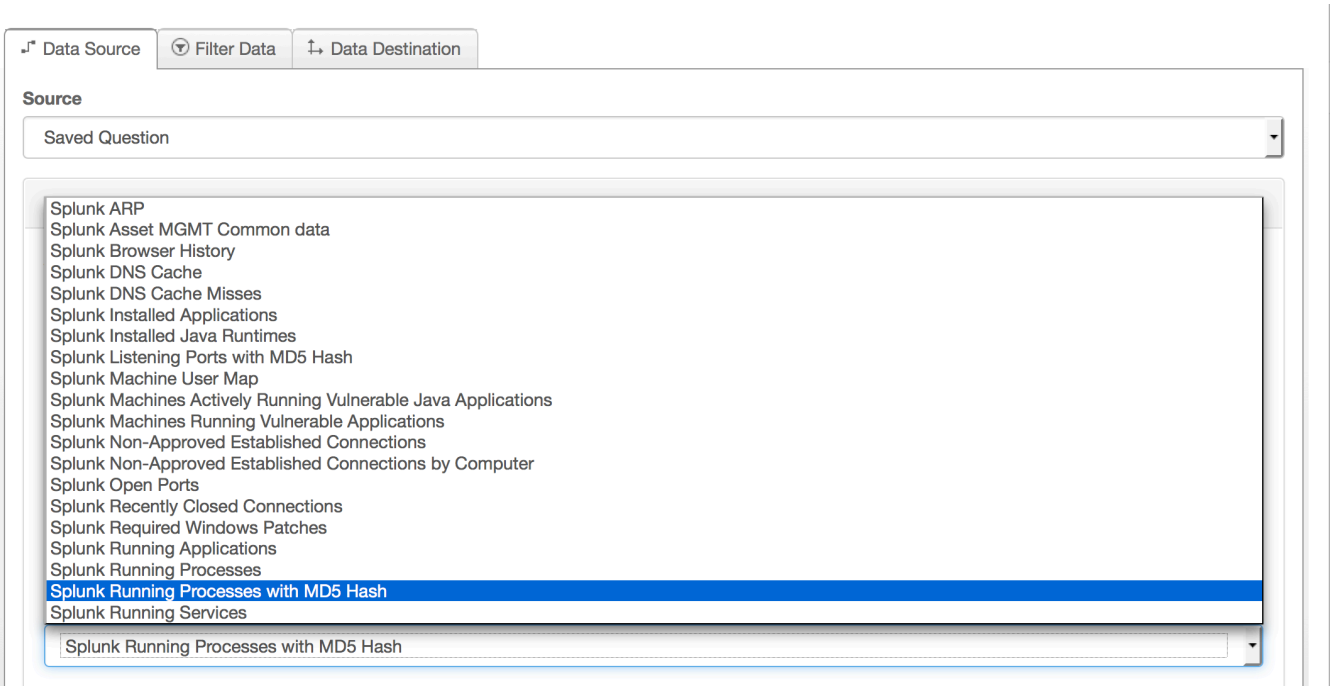




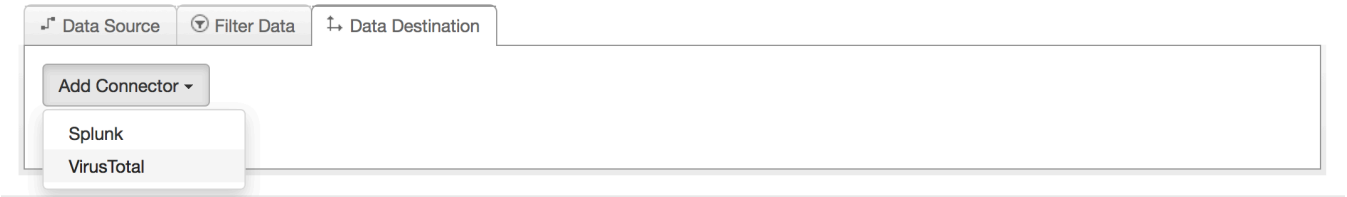
2. Enter a Name for the Connection in the Name field
3. In the Source drop-down list, select Saved Question
4. Select All Computers from the Computer Group drop-down.



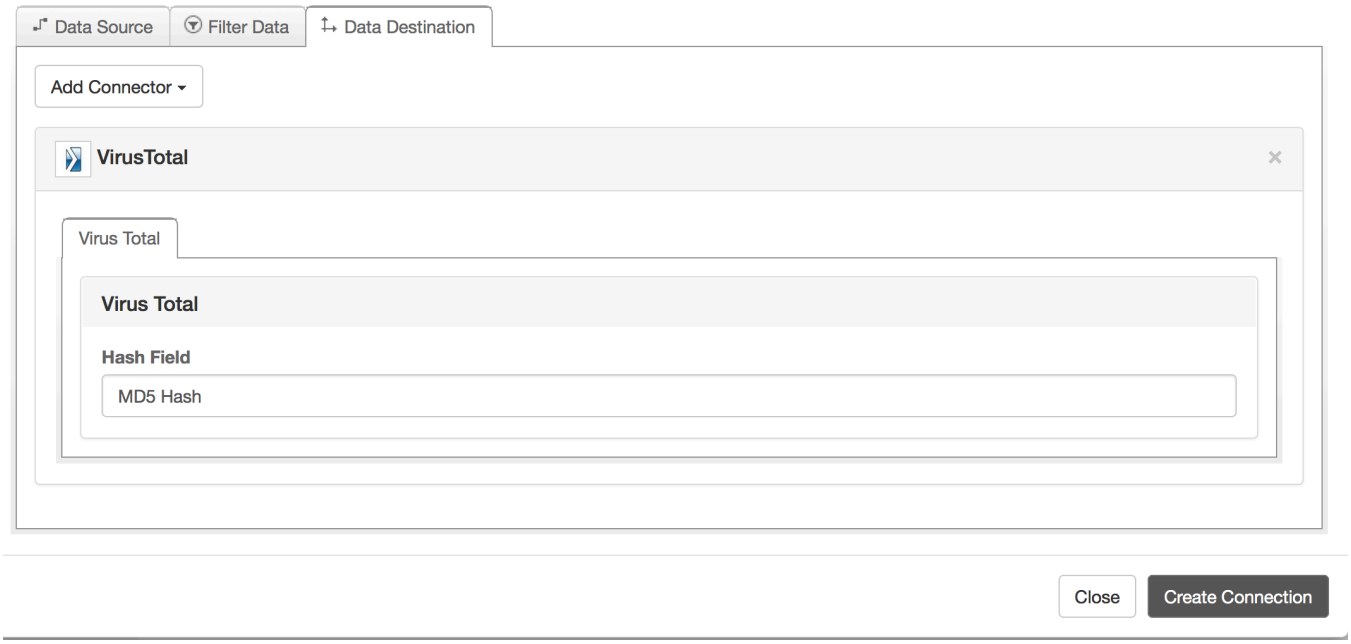
5. In the Saved Question Name, type Splunk and then scroll down and select Splunk Running Processes with MD5 Hash



At this point you may want to adjust the frequency this question is asked. The default 1 Hour interval is adequate. You can also select to target a specific Computer Group by selecting a defined computer group if want to limit the question target.



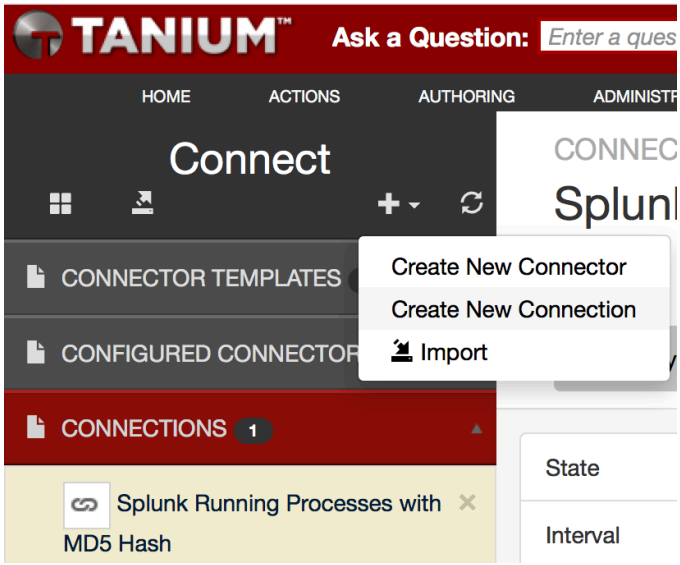
6. Select the Data Destination tab; Select the VirusTotal from the Add Connector drop-down list.

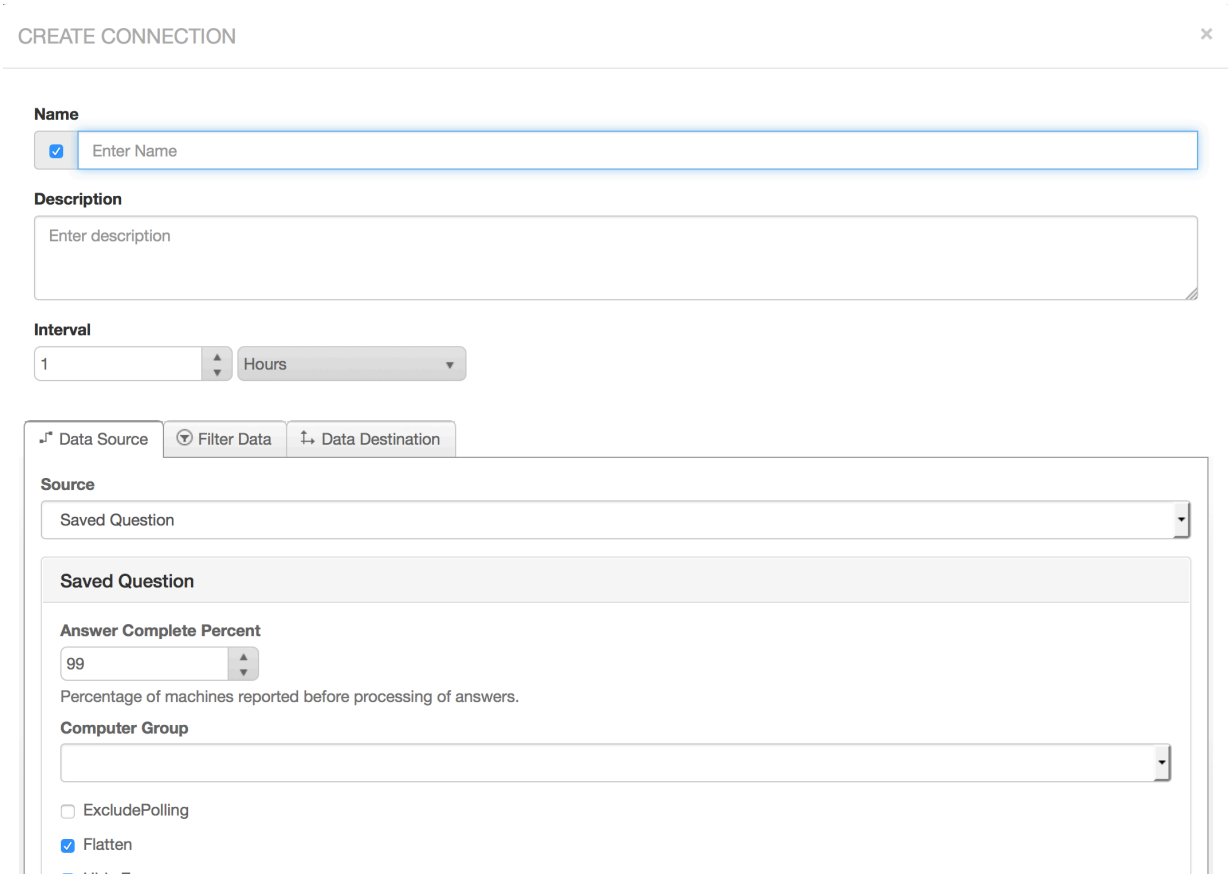


7. Click Create Connection

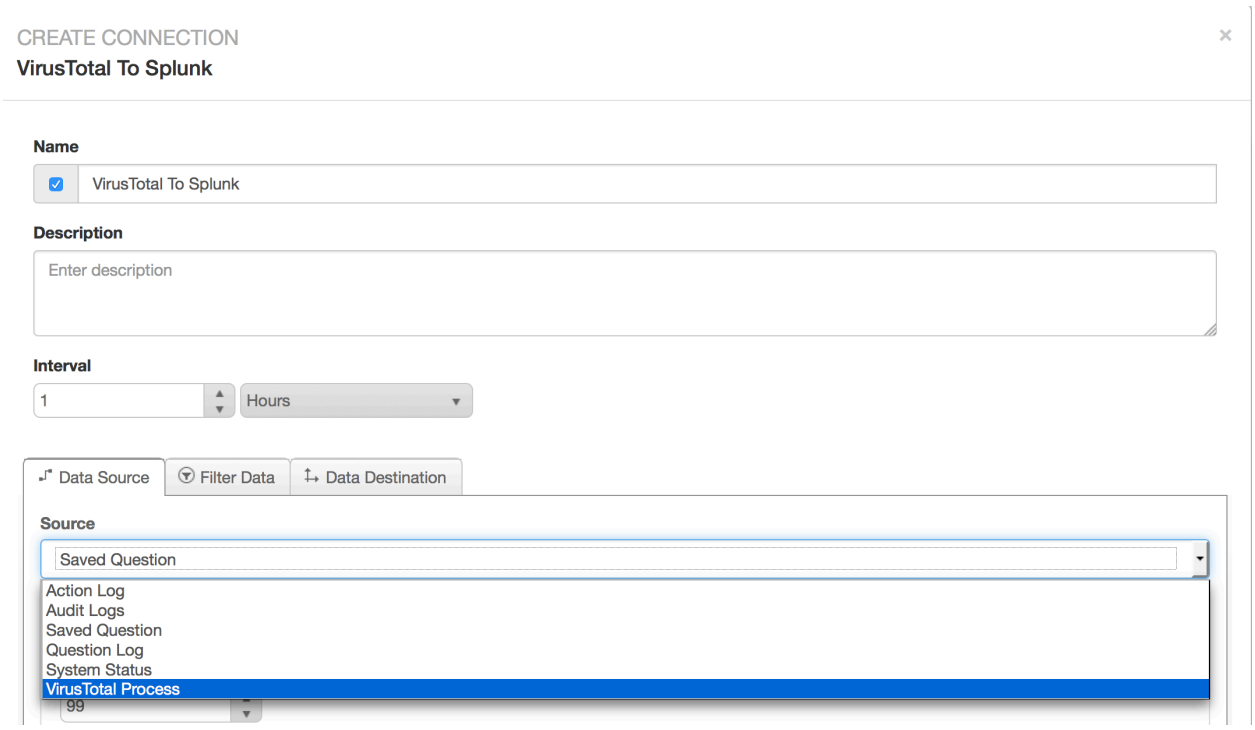
At this point you have created the Connection (Splunk Running Process with MD5 Hash) that will feed the VirusTotal Connector. Now you will need to create the Connection to receive the MD5 hashes, send them to VirusTotal, and then forward the VirusTotal results to Splunk.

1. From the Connect pane, click on the "+" and select Create New Connection.

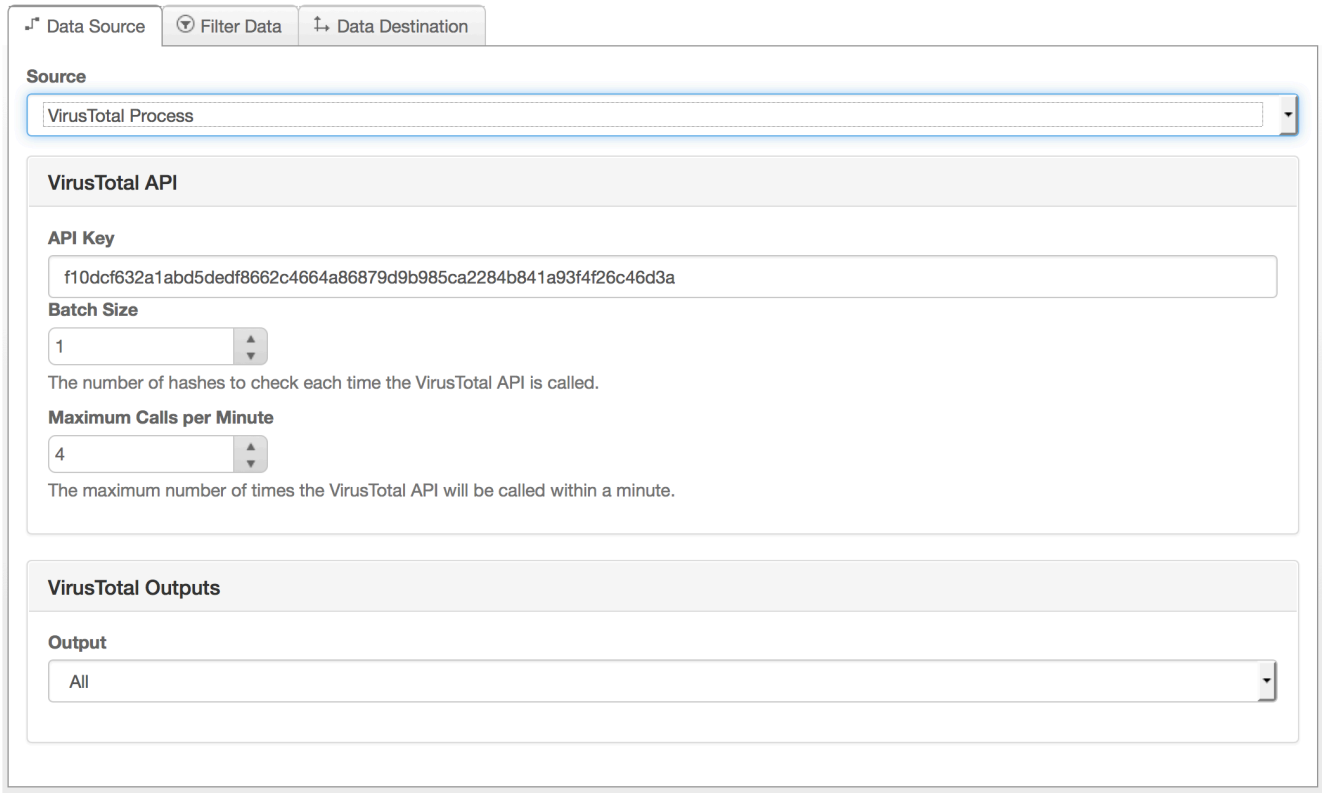




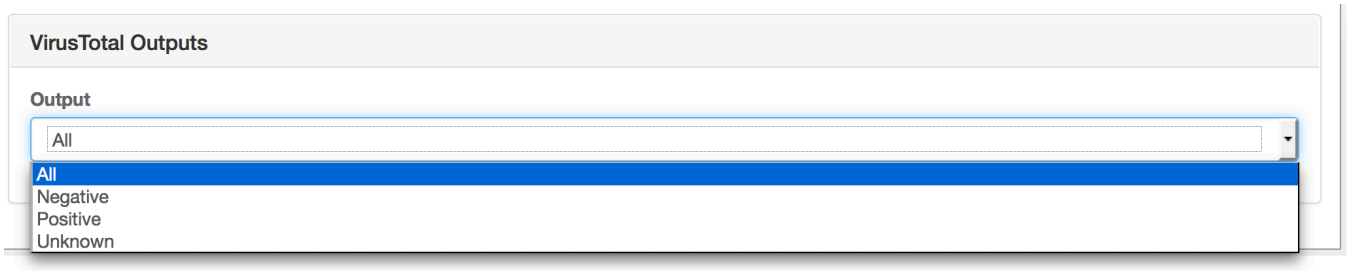
2. Enter a name for the Connection. e.g. VirusTotal Process to Splunk
3. For Source expand the drop-down list, scroll down and select VirusTotal Process.



4. In the API Key field, enter your VirusTotal API key.

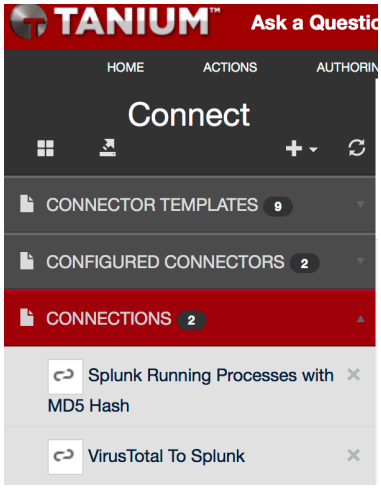


5. Choose the type of VirusTotal results to output.



6. Select the Data Destination tab
7. Expand Add Connector, select Splunk

8. Click Create Connection

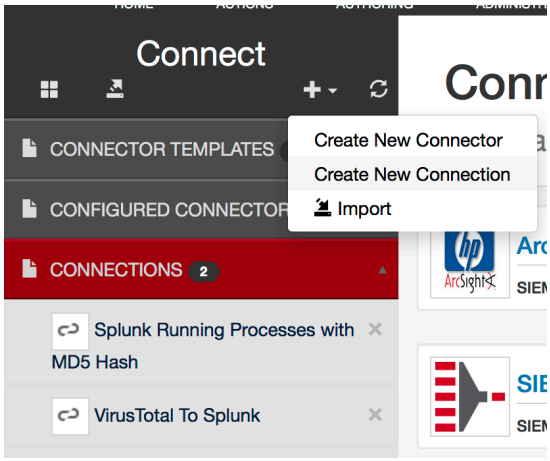


You have now configured the Splunk Running Processes with MD5 Hash question to forward the MD5 Hash results to VirusTotal Connector. The VirusTotal Process Connection receives the MD5 hashes from the VirusTotal Connector, buffers and sends the hashes to VirusTotal. The VirusTotal results are then forwarded to Splunk.

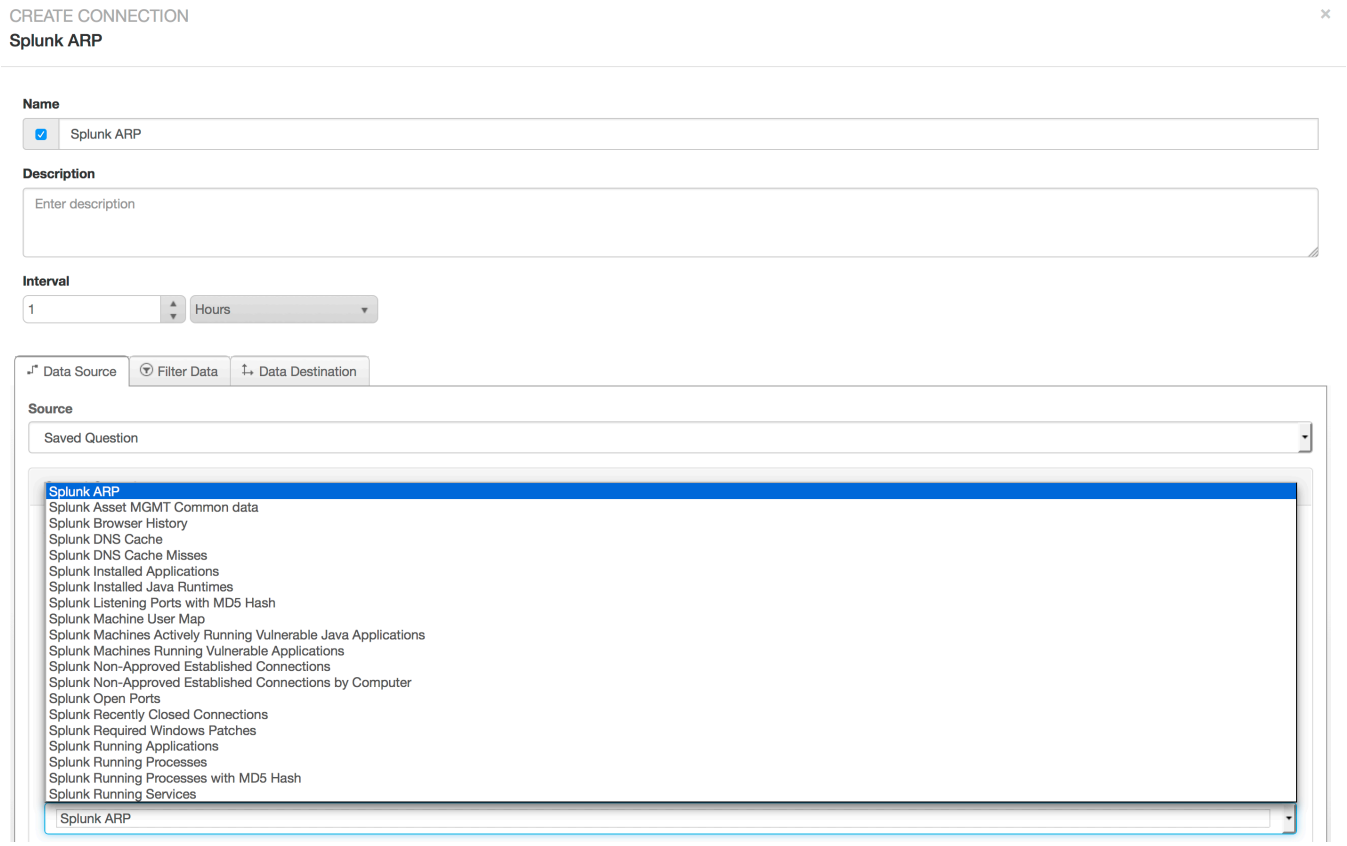
Adding additional Splunk Saved questions

In this section, you will add the rest of the Splunk saved questions.

1. From the Connect pane, click on the "+" and select Create New Connection.

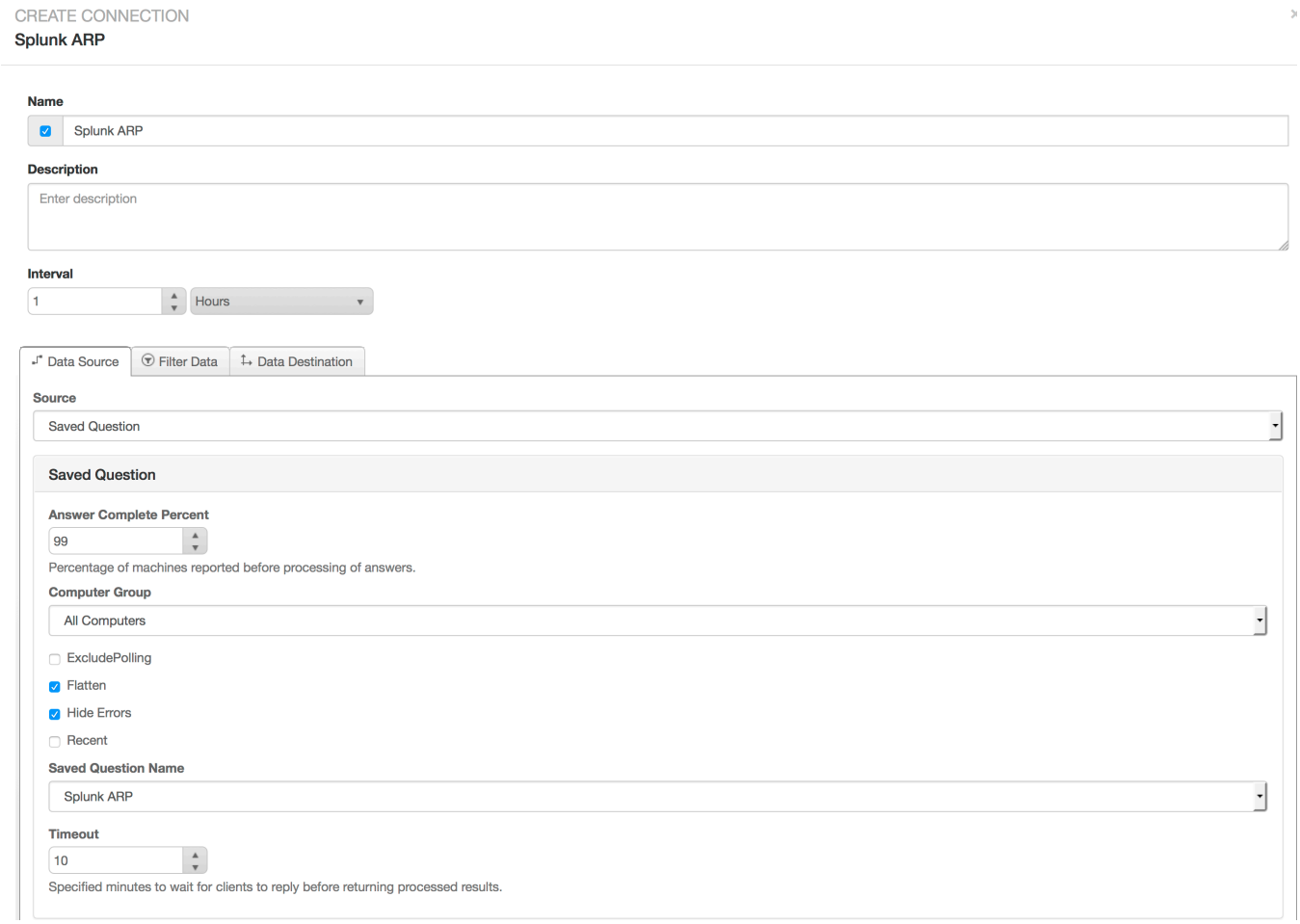


2. Enter a Name for the Connection
3. Select Saved Question as the Source
4. In the Save Question Name, type Splunk. Scroll down and select Splunk ARP

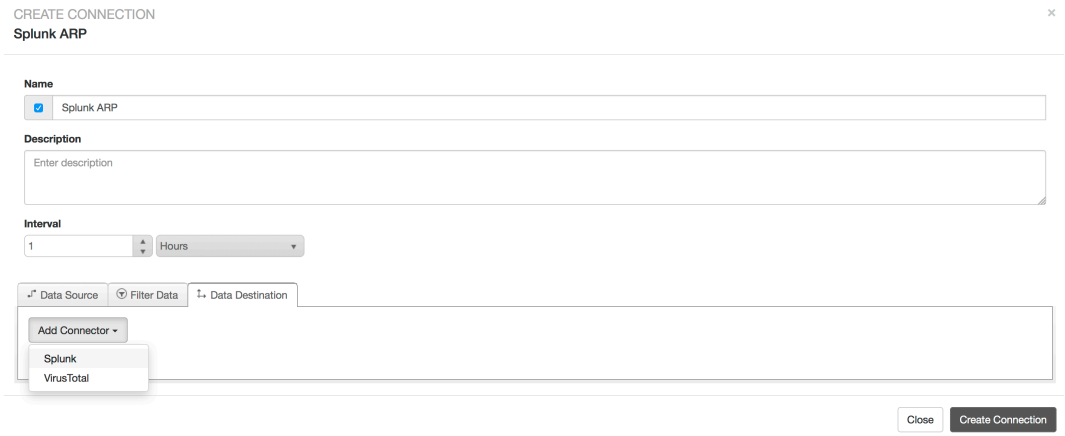


5. Select Computer Group.

At this point you may want to adjust the frequency this question is asked. The default 60 minutes frequency is adequate.

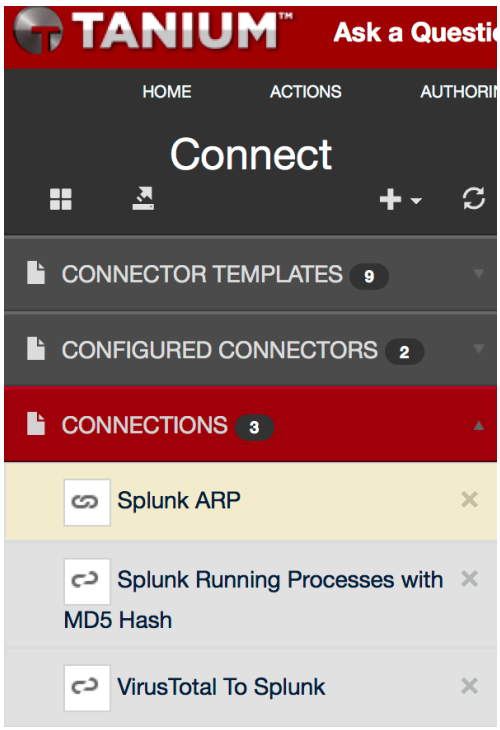


6. Click on the Data Destination tab



7. From the Add Connector drop-down list, select Splunk

8. Click Create Connection



Repeat the above steps until you have added all of the Splunk saved questions

When you have completed adding all of the questions, your panel should look like this.