

2015

Tanium: Splunk Application

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



TANIUM™

Contents

Introduction	1
Installation.....	1
Installing the Tanium Splunk Application.....	1
Adding a Data Input for Tanium.....	2
Importing Splunk Application Saved Questions thru the Tanium Console	3
Configuring Splunk Connector in Tanium Connect	4
Configuring VirusTotal Connector in Tanium Connect.....	7
Adding Splunk Saved Questions in Tanium Connect.....	9
Adding Splunk Running Processes with MD5 Hash question for VirusTotal Connector.....	9
Adding additional Splunk Saved questions.....	17

© 2015 Tanium Inc.

The Tanium logo is a trademark of Tanium Inc. All rights reserved.
All other trademarks are property of their respective owners.

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.

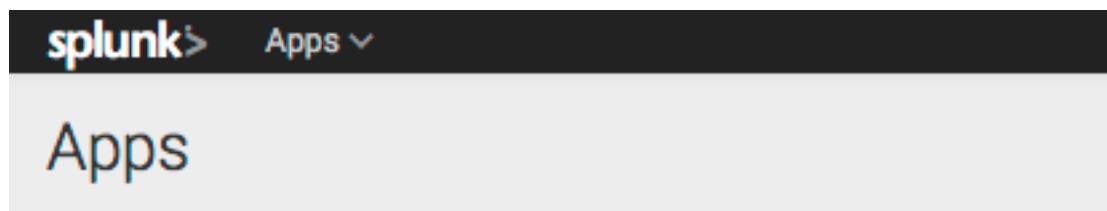
The Tanium Splunk Application contains a set of dashboards that correspond to a fixed set of questions that populate the data. The dashboards display critical software vulnerabilities, unmanaged assets, application and process visibility, detailed asset management information, suspicious open ports and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

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

[Browse...](#) No file selected.

Upgrade app. Checking this will overwrite the app if it already exists.

[Cancel](#)

[Upload](#)

Today	▲	Date Modified	Size
 tanium.spl		2:14 PM	4 KB

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.

Tanium

[Dashboards](#)

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.

Source

TCP port *

9081

Accept connections from all hosts?

 Yes No, restrict to one host

Source name override

*If set, overrides the default source value for your TCP entry (host:port).***Source type**

Set sourcetype field for all events from this source.

Set sourcetype *

Source type

If this field is left blank, the default value of tcp-raw will be used for the source type. [More settings](#)[Cancel](#)[Save](#)

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.

The screenshot shows the Tanium Console homepage. At the top, there's a navigation bar with links for HOME, ACTIONS, AUTHORING, ADMINISTRATION, and DEPLOY CLIENTS. The AUTHORING link is highlighted in red. On the right side of the header, there are links for PREFERENCES and LOGOUT. Below the header, there's a search bar labeled "Ask a Question:" with the placeholder text "Enter a question here. Tanium understands plain English." To the right of the search bar are buttons for PREFERENCES and LOGOUT. The main content area is currently empty.

1. Select Authoring.

The screenshot shows the Tanium Console Authoring page. The navigation bar at the top has the AUTHORING link highlighted in red. Below the header, there are tabs for Dashboards, Saved Questions, Sensors, and Packages. The "Saved Questions" tab is active. On the right side, there's a button labeled "Import Content..." with a red exclamation mark icon. The main content area is currently empty.

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

Today	Date Modified	Size	Kind
Splunk saved_questions.xml	1:52 PM	393 KB	XM...ent

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.

The screenshot shows the Tanium Connect interface with the 'CONNECT' tab selected. On the left, there's a sidebar with 'CONNECTOR TEMPLATES' (9), 'CONFIGURED CONNECTORS' (0), and 'CONNECTIONS' (0). The main area is titled 'Connector Templates' and displays nine available templates:

- ArcSight (SIEM)
- Email Results (Utility)
- Json To File (Utility)
- LogRhythm (SIEM)
- McAfee SIEM (SIEM)
- Splunk (SIEM)
- VirusTotal (Threat)
- Write To File (Utility)

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

The screenshot shows the Tanium Connect interface with the 'CONNECT' tab selected. On the left, there's a sidebar with 'CONNECTOR TEMPLATES' (9), 'CONFIGURED CONNECTORS' (0), and 'CONNECTIONS' (0). A context menu is open over the 'CONNECTOR TEMPLATES' item, showing the following options:

- Create New Connector
- Create New Connection
- Import

- Expand the Create Connector from this template, scroll down and select Splunk

Create Connector

X

Create connector from this template:

ArcSight

ArcSight
Email Results
Json To File
LogRhythm
McAfee SIEM
SIEM
Splunk
VirusTotal
Write To File

3. Click Next.

CREATE CONNECTOR

Splunk

splunk>

Name

Description

Delimiter-separated values

Delimiter Settings

Separator

Settings

Name Escape

Name Escape Replace

Value Escape

Value Escape Replace

4. Click on the Convert to Logs button.

CREATE CONNECTOR

Splunk**Name**

Splunk

Description

Enter description

Convert to Logs **Send To Splunk**

Delimiter-separated values

Delimiter-separated values

Json

Syslog (RFC5424)

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

CREATE CONNECTOR

Splunk**Name**

Splunk

Description

Enter description

Convert to Logs **Send To Splunk**

Rotating Log Files

Rotating Log Files

TCP

UDP

7. Select TCP Receiver from the drop-down list

[Convert to Logs](#) [Send To Splunk](#)

TCP

Settings

Host

172.16.21.12

Port

9081



The port the receiver service is listening on.

Separator

\n

[Close](#)

[Create connector](#)

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

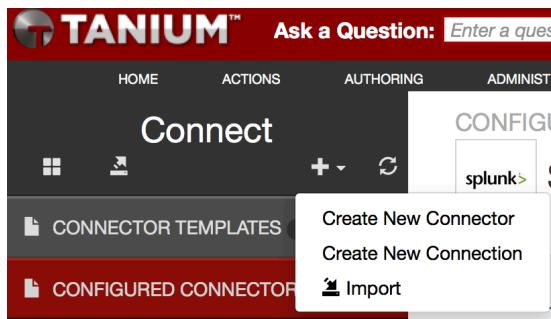
You will now see the Splunk Connector in the Configured Connectors Pane

The screenshot shows the Tanium Connect interface. The top navigation bar includes links for HOME, ACTIONS, AUTHORIZING, CONNECT (which is selected), and IOC DETECT. A red banner at the top says "Ask a Question: Enter a question here. You can use plain English." On the left, there's a sidebar with "CONNECT" and sections for "CONNECTOR TEMPLATES" and "CONFIGURED CONNECTORS". Under "CONFIGURED CONNECTORS", there is one item named "Splunk". The main pane is titled "CONFIGURED CONNECTOR" and shows a summary for the "Splunk" connector. It includes fields for "Host" (172.16.21.12), "Port" (9081), and "Separator" (\n). At the bottom of this pane are buttons for "Convert to Logs" and "Send To Splunk". On the far right, there are icons for "Export", "Edit", and "Delete".

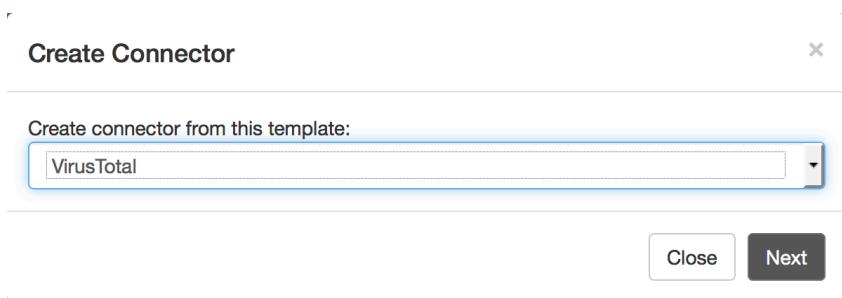
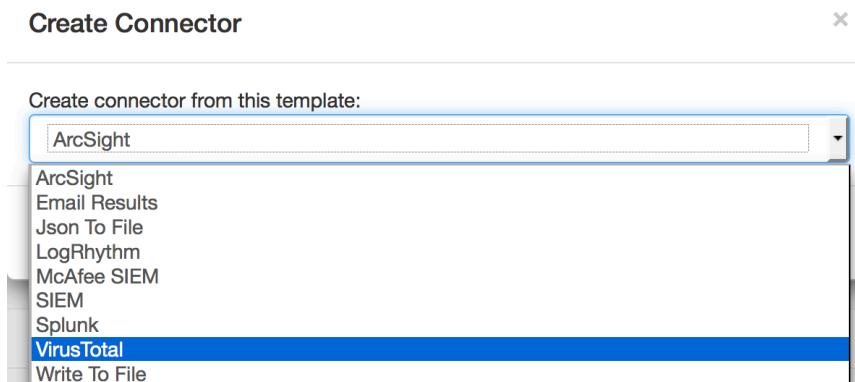
Configuring VirusTotal Connector in Tanium Connect

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.

CREATE CONNECTOR



VirusTotal

X

Name

VirusTotal

Description

Enter description

Virus Total

Virus Total

Hash Field

MD5 Hash

Close

Create connector

4. Click Create Connector

The screenshot shows the Tanium Connect interface. At the top, there's a navigation bar with tabs: HOME, ACTIONS, AUTHORIZING, ADMINISTRATION, CONNECT (which is highlighted), and IOC DETECT. Below the navigation bar, there's a search bar labeled "Ask a Question: Enter a question here. You can use plain English." and a "LOGOUT" button. The main area is titled "CONFIGURED CONNECTOR" and shows a connector named "VirusTotal". On the left side, there's a sidebar titled "Connect" with sections for "CONNECTOR TEMPLATES" (Splunk) and "CONFIGURED CONNECTORS" (Splunk, VirusTotal). The "VirusTotal" connector is selected and highlighted in yellow. On the right side, there are buttons for "Export" and "Edit". A vertical toolbar on the far right includes icons for settings, export, and help.

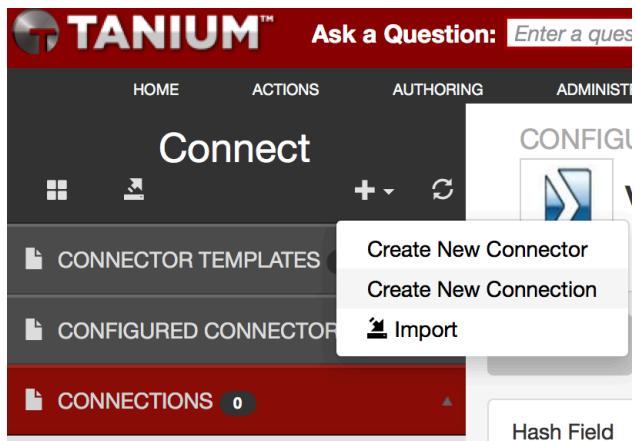
You have now successfully configured the VirusTotal Connector.

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

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



CREATE CONNECTION

Name

 Enter Name

Description

Enter description

Interval

1 Hours

 Data Source Filter Data Data Destination

Source

Saved Question

Saved Question

Answer Complete Percent

99

Percentage of machines reported before processing of answers.

Computer Group

 ExcludePolling Flatten

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.

CREATE CONNECTION

Splunk Running Processes with MD5 Hash

Name

Splunk Running Processes with MD5 Hash

Description

Enter description

Interval

1

Hours

Data Source

Filter Data

Data Destination

Source

Saved Question

Saved Question**Answer Complete Percent**

99

Percentage of machines reported before processing of answers.

Computer Group

All Computers

 ExcludePolling Flatten Hide Errors Recent

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

Saved Question

- Splunk ARP
- Splunk Asset MGMT Common data
- Splunk Browser History
- Splunk DNS Cache
- Splunk DNS Cache Misses
- Splunk Installed Applications
- Splunk Installed Java Runtimes
- Splunk Listening Ports with MD5 Hash
- Splunk Machine User Map
- Splunk Machines Actively Running Vulnerable Java Applications
- Splunk Machines Running Vulnerable Applications
- Splunk Non-Approved Established Connections
- Splunk Non-Approved Established Connections by Computer
- Splunk Open Ports
- Splunk Recently Closed Connections
- Splunk Required Windows Patches
- Splunk Running Applications
- Splunk Running Processes
- Splunk Running Processes with MD5 Hash**
- Splunk Running Services

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.

Add Connector ▾

- Splunk
- VirusTotal**

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

The screenshot shows the Tanium interface with a red header bar. Below it is a white search bar with three buttons: 'Data Source', 'Filter Data', and 'Data Destination'. Underneath is a button labeled 'Add Connector'. A modal window titled 'VirusTotal' is open, displaying a 'Virus Total' connector configuration. It has a 'Hash Field' section with 'MD5 Hash' selected. At the bottom right of the modal are 'Close' and 'Create Connection' buttons.

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.

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

The screenshot shows the Tanium interface with a dark-themed 'Connect' pane. On the left, there are sections for 'CONNECTOR TEMPLATES', 'CONFIGURED CONNECTORS', and 'CONNECTIONS' (1). The 'CONNECTIONS' section contains a card for 'Splunk Running Processes with MD5 Hash'. A context menu is open over this card, listing 'Create New Connector', 'Create New Connection', and 'Import'. The 'Create New Connection' option is highlighted. The background shows other parts of the Tanium interface, including a navigation bar with 'HOME', 'ACTIONS', 'AUTHORING', and 'ADMINISTRATOR' tabs.

CREATE CONNECTION

X

Name

Enter Name

Description

Enter description

Interval

1 Hours

Source

Saved Question

Saved Question

Answer Complete Percent

99

Percentage of machines reported before processing of answers.

Computer Group

ExcludePolling

Flatten

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.

CREATE CONNECTION

VirusTotal To Splunk

Name
 VirusTotal To Splunk
Description

Enter description

Interval

1 Hours

 Data Source Filter Data Data Destination
Source

Saved Question

Action Log
Audit Logs
Saved Question
Question Log
System Status
VirusTotal Process
99

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

 Data Source Filter Data Data Destination
Source

VirusTotal Process

VirusTotal API**API Key**

f10dcf632a1abd5dedf8662c4664a86879d9b985ca2284b841a93f4f26c46d3a

Batch Size

1

The number of hashes to check each time the VirusTotal API is called.

Maximum Calls per Minute

4

The maximum number of times the VirusTotal API will be called within a minute.

VirusTotal Outputs**Output**

All

5. Choose the type of VirusTotal results to output.

VirusTotal Outputs**Output**

All

All
Negative
Positive
Unknown

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

The screenshot shows the 'Data Destination' tab interface. At the top, there are three buttons: 'Data Source', 'Filter Data', and 'Data Destination'. Below these, a dropdown menu labeled 'Add Connector' is open, displaying two options: 'Splunk' and 'VirusTotal'. The 'Splunk' option is highlighted.

The screenshot shows the 'Data Destination' tab interface. At the top, there are three buttons: 'Data Source', 'Filter Data', and 'Data Destination'. Below these, a dropdown menu labeled 'Add Connector' is open, displaying one option: 'Splunk'. The 'Splunk' option is highlighted and selected.

Create Connection

8. Click Create Connection

The screenshot shows the 'Connect' page interface. At the top, there are navigation links: 'HOME', 'ACTIONS', and 'AUTHORITY'. Below this is a search bar and a 'Connect' button. The main area is titled 'Connections' and contains two entries:

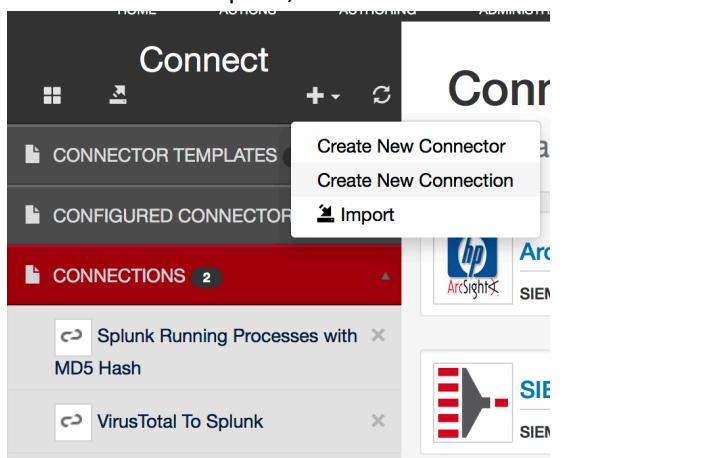
- Splunk Running Processes with MD5 Hash
- VirusTotal To Splunk

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.

- From the Connect pane, click on the “+” and select Create New Connection.



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

CREATE CONNECTION

Splunk ARP

Name
 Splunk ARP

Description

Interval

Source

Saved Questions

- Splunk ARP**
- Splunk Asset MGMT Common data
- Splunk Browser History
- Splunk DNS Cache
- Splunk DNS Cache Misses
- Splunk Installed Applications
- Splunk Installed Java Runtimes
- Splunk Listening Ports with MD5 Hash
- Splunk Machine User Map
- Splunk Machines Actively Running Vulnerable Java Applications
- Splunk Machines Running Vulnerable Applications
- Splunk Non-Approved Established Connections
- Splunk Non-Approved Established Connections by Computer
- Splunk Open Ports
- Splunk Recently Closed Connections
- Splunk Required Windows Patches
- Splunk Running Applications
- Splunk Running Processes
- Splunk Running Processes with MD5 Hash
- Splunk Running Services

Save Question

- Select Computer Group.

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

CREATE CONNECTION
Splunk ARP

Name
 Splunk ARP

Description
Enter description

Interval
1 Hours

Data Source Filter Data Data Destination

Source
Saved Question

Saved Question

Answer Complete Percent
99

Percentage of machines reported before processing of answers.

Computer Group
All Computers

ExcludePolling
 Flatten
 Hide Errors
 Recent

Saved Question Name
Splunk ARP

Timeout
10

Specified minutes to wait for clients to reply before returning processed results.

6. Click on the Data Destination tab

CREATE CONNECTION
Splunk ARP

Name
 Splunk ARP

Description
Enter description

Interval
1 Hours

Data Source Filter Data Data Destination

Add Connector ▾
Splunk VirusTotal

7. From the Add Connector drop-down list, select Splunk**CREATE CONNECTION**
Splunk ARP

Name
 Splunk ARP

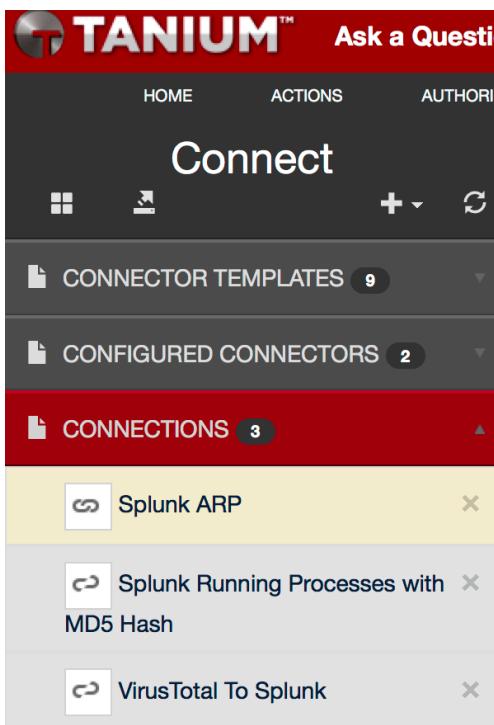
Description
Enter description

Interval
1 Hours

Data Source Filter Data Data Destination

Add Connector ▾
Splunk

8. Click Create Connection



The screenshot shows the Tanium Connect interface. At the top, there are navigation links: HOME, ACTIONS, AUTHORITY, and SUPPORT. Below that is a search bar with the placeholder "Ask a Question". The main area is titled "Connect" and features a toolbar with icons for refresh, add, and filter. On the left, a sidebar lists categories: CONNECTOR TEMPLATES (9), CONFIGURED CONNECTORS (2), and CONNECTIONS (3). The CONNECTIONS section is expanded, showing three items: "Splunk ARP" (highlighted in yellow), "Splunk Running Processes with MD5 Hash", and "VirusTotal To Splunk". Each item has a delete icon to its right.

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.

TANIUM™ Ask a Question

HOME ACTIONS AUTHORITY

Connect

CONNECTOR TEMPLATES 9

CONFIGURED CONNECTORS 2

CONNECTIONS 24

- Splunk ARP
- Splunk Asset MGMT Common Data
- Splunk Browser History
- Splunk DNS Cache
- Splunk DNS Cache Misses
- Splunk Installed Applications
- Splunk Installed Java Runtimes
- Splunk Listening Ports with MD5 Hash
- Splunk Machine User Map
- Splunk Machines Actively Running Vulnerable Java Applications
- Splunk Machines Running Vulnerable Applications
- Splunk Non-Approved

