Palo Alto Traps Custom Content for Tanium

Abstract:

This document will describe the components of the Palo Alto Networks Traps Custom Content for Tanium, its basic usage and maintenance.

Introduction:

The PAN Traps Tanium Custom Content is a collection of functionality to install Traps and query the state of the Traps system. Tanium's peer to peer communication will be the platform for the systems administrator to manage the Traps install. The Traps custom content will use this peer to peer communication for bootstrapping the Traps installer as well as a management communications platform for querying and extracting Traps current state.

Installing The Custom Content:

The Traps Custom Content is broken down in to several xml files. Namely

Palo Alto Networks Traps Sensors.xml
Palo Alto Networks Traps Dashboard.xml
Palo Alto Networks Traps Packages.xml
Palo Alto Networks Traps Saved Questions.xml

To install the Traps content via the Tanium console select Authoring then “Import form xml” and select each xml file. An alternative is to install the single file named

Palo Alto Traps Combined Content.xml

which contains all the content of the above files concatenated together with a header. On import the Tanium system will ask for confirmation to install the custom content. Confirm the install and the content will be installed.

Traps Installation (a Persistent Tanium action):

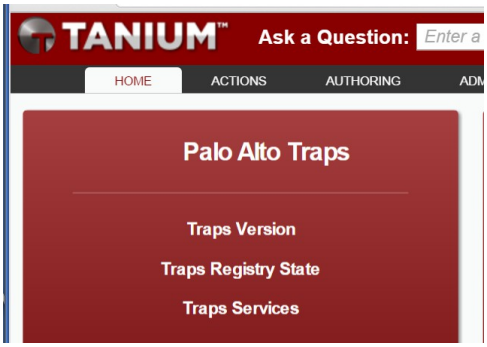
The custom content components are broken down in to two logical groupings. The first logical grouping is the persistent action of installing traps on endpoints. The second logical grouping is the transient action on getting the sate of Traps on the endpoints.

The persistent action of installing is based on a Tanium action is a “package”. The Traps installer package is one of two install actions. The two separate actions are either install the x86 or x64 version of the Traps software. Under Authoring, Packages select the Traps 64 bit installer and click the pencil to edit. Under the files section use the open file dialogue to add the 64 bit file. An alternative is to select a URI rather a file path. Follow this same procedure for the x86 install. To install the Traps system, ask a question on the main Tanium search bar, like “Get Computer Name and x64/x86? from all machines”, select all 64 bit or exclusively x86 bit computers, right click and select perform action. Select the install Traps action and select the x86 or 64 installer. See the Tanium kb for more details of performing actions. On actions creation there will be two parameters, one for the Traps server and the other for SSL option. The SSL option will default to on. Enter the Traps server to install and config the endpoint right away.

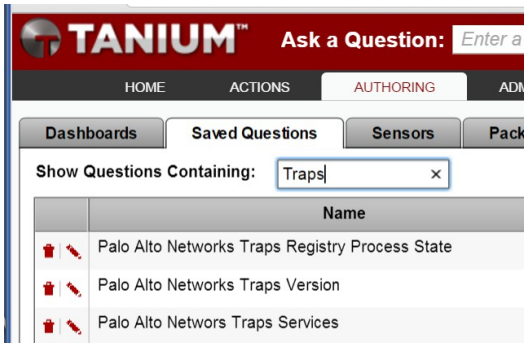
Dashboards, Saved Questions, Sensors (a Transient State Fetch via Tanium):

The remaining transient state querying parts of the custom content are the dashboard, sensors and the saved questions. In short the dashboard provides a simple one click interface to query the Traps state, the saved questions compose the verbage of the dashboard and the sensor is the programmed logic behind the verbage.

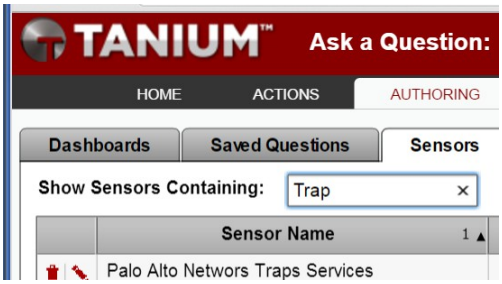
Dashboard



Saved Question



Sensors



The dashboard is presented on the Tanium console home screen, and provides a single click interface to the saved questions. Simply click to use. For example if you want to know which versions are installed click on “Traps Version”. The remaining dashboard questions such as Traps services will return a hostname and a list of running Traps services on the endpoint. The Traps registry state will check the registry key “HKLM\System\Cyvera\Policy\Organization\Process\Default” to see if Traps is running. The saved questions are not directly accessible and are only useable via the one click option on the dashboard. The sensor is accessible via the main NLP search bar and will check the running traps services. To see an example enter the query “get computer name and traps services”. The running traps services will respond along with the hostname.

Modifying or Creating New Custom Content:

All creation or modification of the custom content is done under the Tanium “Authoring” tab and is broken down the same way as Dashboard, Saved Questions, Sensors, Packages. The Dashboard is composed of a single panel made of the Traps saved questions. Simply add any new saved question to the dashboard with the “+” option. Saved questions are saved verbage in the same way one would type it in the NLP search bar. To see what the saved question is select, saved question, choose the question of interest and select the pencil. The Traps sensor is a WMI query. To view the WMI query,

under authoring, then sensors click the pencil to view the query. Note that all of the Traps content, saved questions, sensors, action packages are name spaced as “Palo Alto Traps”. As always, be sure to back up the system before making any changes, always save your work and test the changes you have made by running the dashboard or asking a Tanium NLP question.

As described earlier, the traps content is divide in to several files namely

Palo Alto Networks Traps Sensors.xml
Palo Alto Networks Traps Dashboard.xml
Palo Alto Networks Traps Packages.xml
Palo Alto Networks Traps Saved Questions.xml

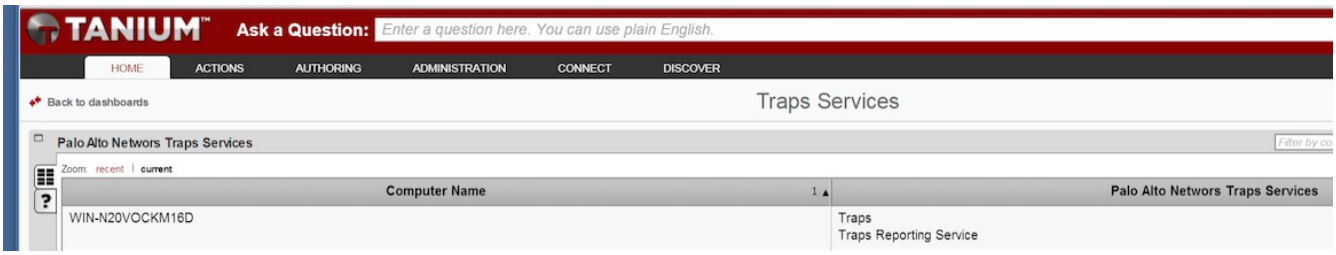
Each file contains the corresponding parts as it is named. For example Palo Alto Traps Dashboard.xml contains the dashboard, ...Packages.xml contains the packages, etc. After making a change to the content, say for a sensor, go to authoring, sensor, new sensor, create the sensor and save it. Select all the traps sensors and click export and choose the above name “*Palo Alto Networks Traps Sensors.xml*”.

Also, described earlier was the ability to have all the separate xml files contained in a single package. The method of creating a single xml file that has all the content in one bundle is as follows. Included in the Traps content zip is a xml bundle header. Update the data in the header, such as version, concatenate all the remaining content and end this file with the xml tag “</content>”.

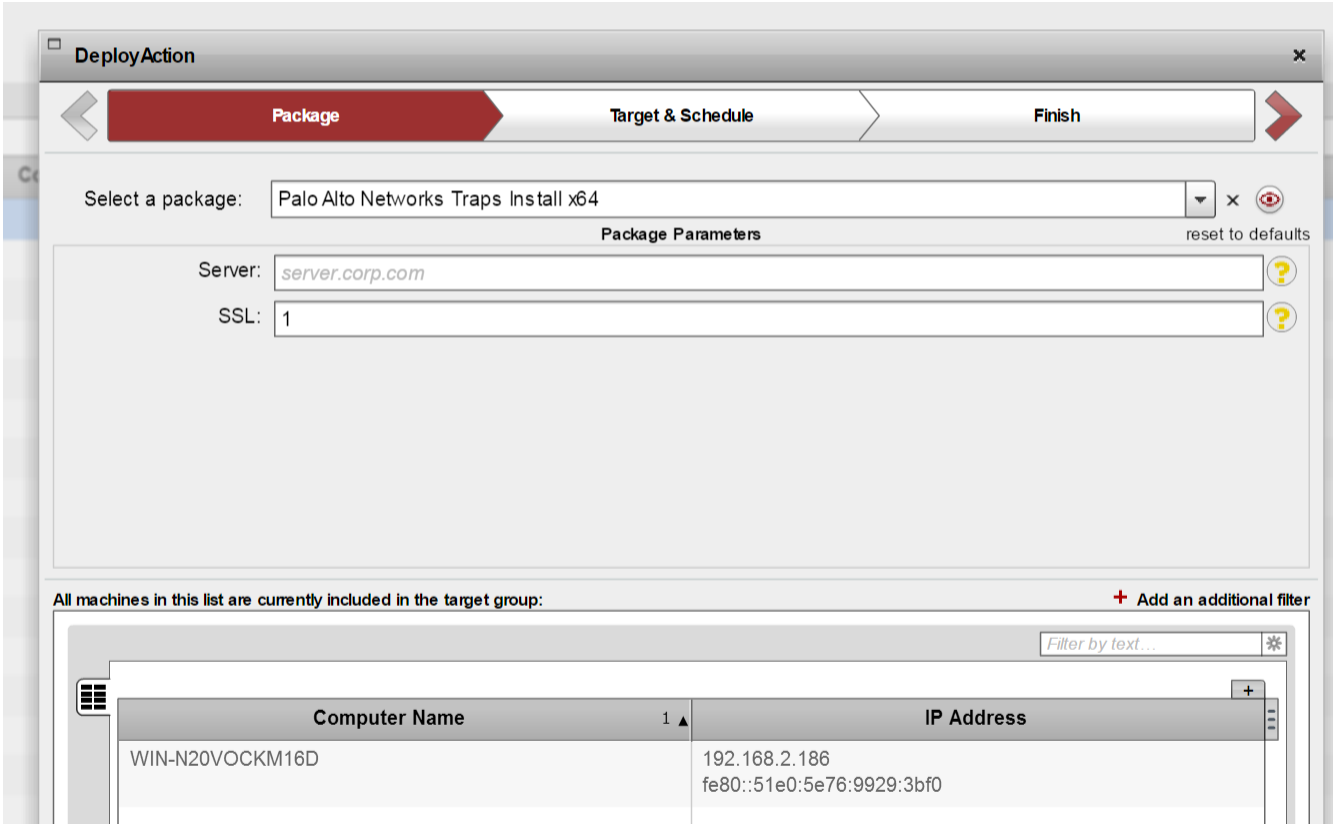
The Traps Sensor contains one sensor that is a WMI query. The query will fetch the name of the running Traps services.

Examples:

To check the Traps running services, click on the “Traps Services” link in the dashboard. After Tanium completes its run, the following will be presented on screen.



To install Traps ask a Tanium question like “computer name and 64”. Once the search is complete highlight all 64bit computers and right click, deploy action, and choose Traps 64 bit install.



More information:

For more information on content creation and Tanium usage please visit the following links.

kb.tanium.com
community.tanium.com