Netsurion™ | EventTracker

Enhancement in Log Search and System Manager

Publication Date: May 6, 2019

Abstract

This document provides enhancements in EventTracker v9.0 log search result and system manager.

Audience

EventTracker v9.0 user(s) who wish to refine the log search result by selecting multiple normalized data and also given an option to pivot the log search results, by selecting multiple CIM fields.

Table of Contents

Options to add multiple CIM fields for pivoting

After performing log search, the user can see new enhancements in the log search result window.

User is provided with an option to filter multiple interesting fields for pivoting the log search results.

To perform multiple CIM field for pivoting.

1. Click **"Add multiple fields for Pivoting"**  icon in the **Interesting** field tab.

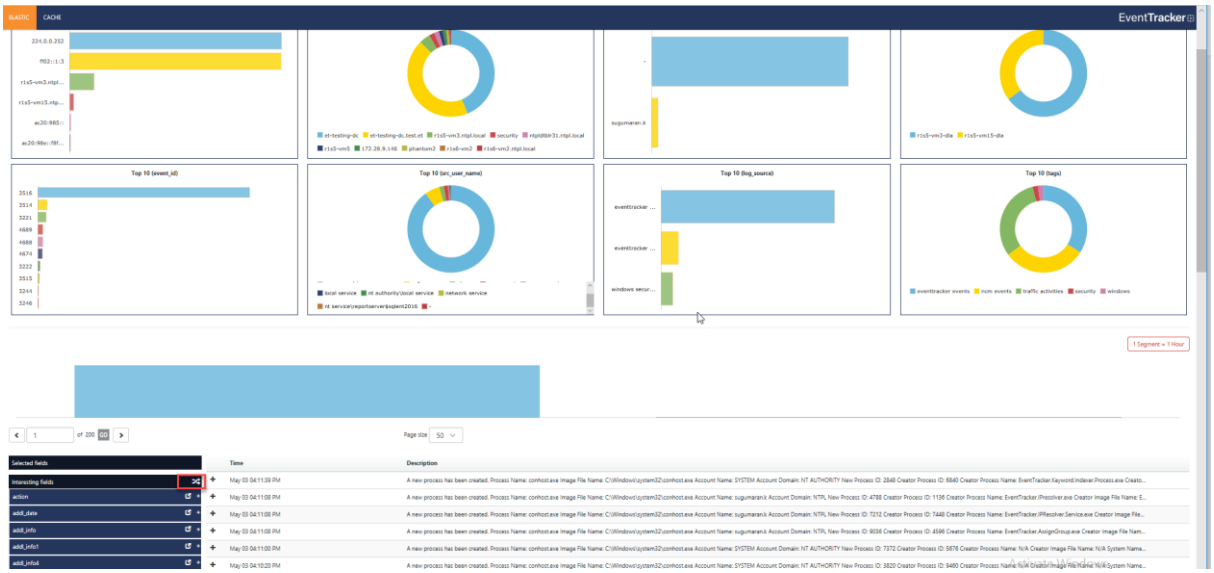

Figure 1

2. **"Add multiple fields for pivoting"** dialog box appears.

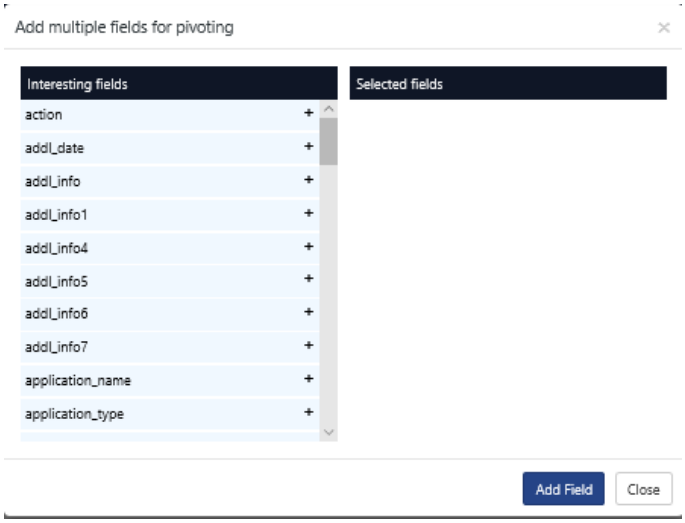

Figure 2

3. Select the CIM fields by clicking **Add field** (**+** sign) icon and click **Add Field** button to add multiple fields for pivoting.

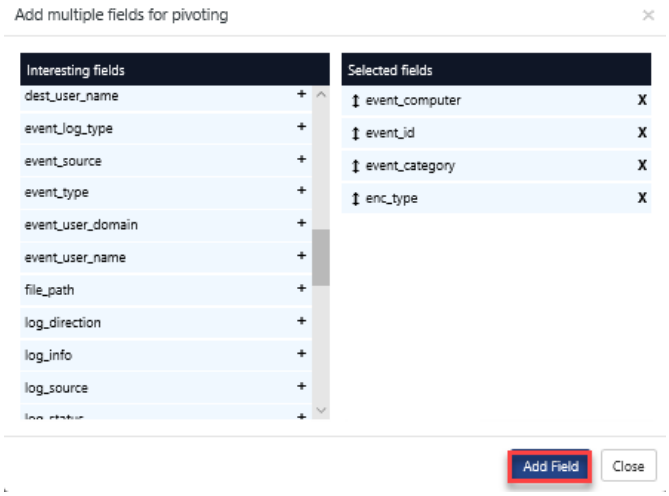

Figure 3

4. The selected fields are displayed in the tabular form as a pivot column as well as under the **Selected field** tab.

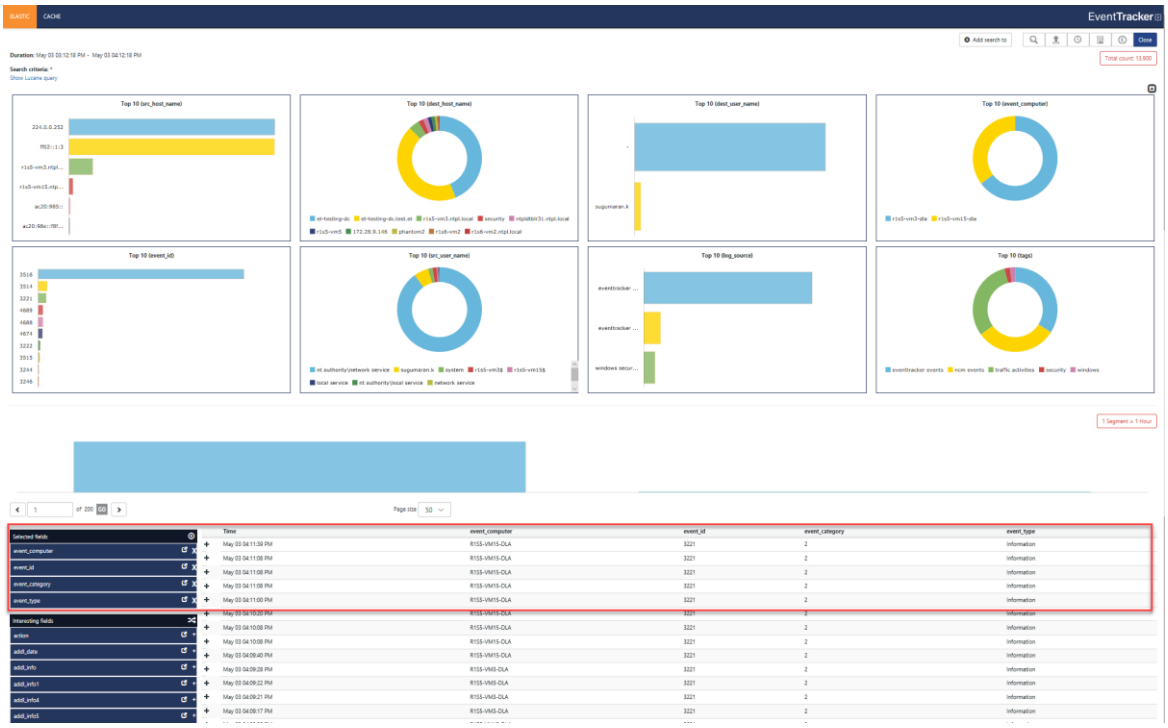

Figure 4

NOTE: The exported log search result file will contain pivoted columns with respect to columns selected for pivoting.

Option to add multiple normalized data by using include/exclude options in log search.

To add the multiple CIM field values or data and get the results based on it

1. Click the **View field values** icon for the respective CIM field. In this example "**event_id"** is chosen.

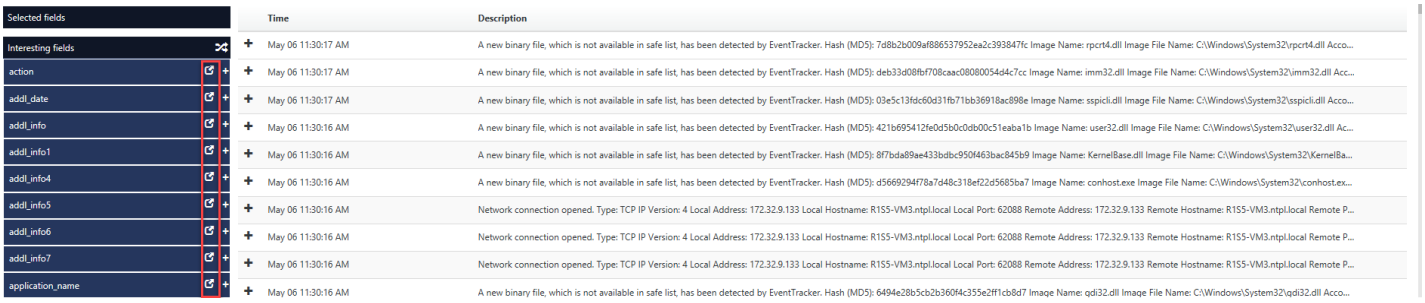

Figure 5

2. Choose the required values to be displayed from the "**Values for event_id"** dialog box window that appears and click **Include**.

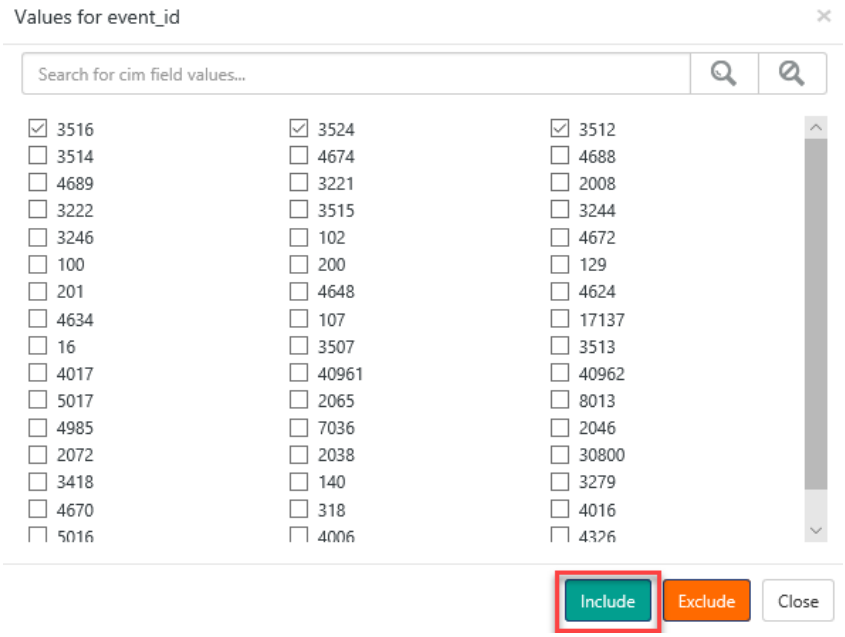

Figure 6

3. The search criteria result displays depending on the values that are selected.

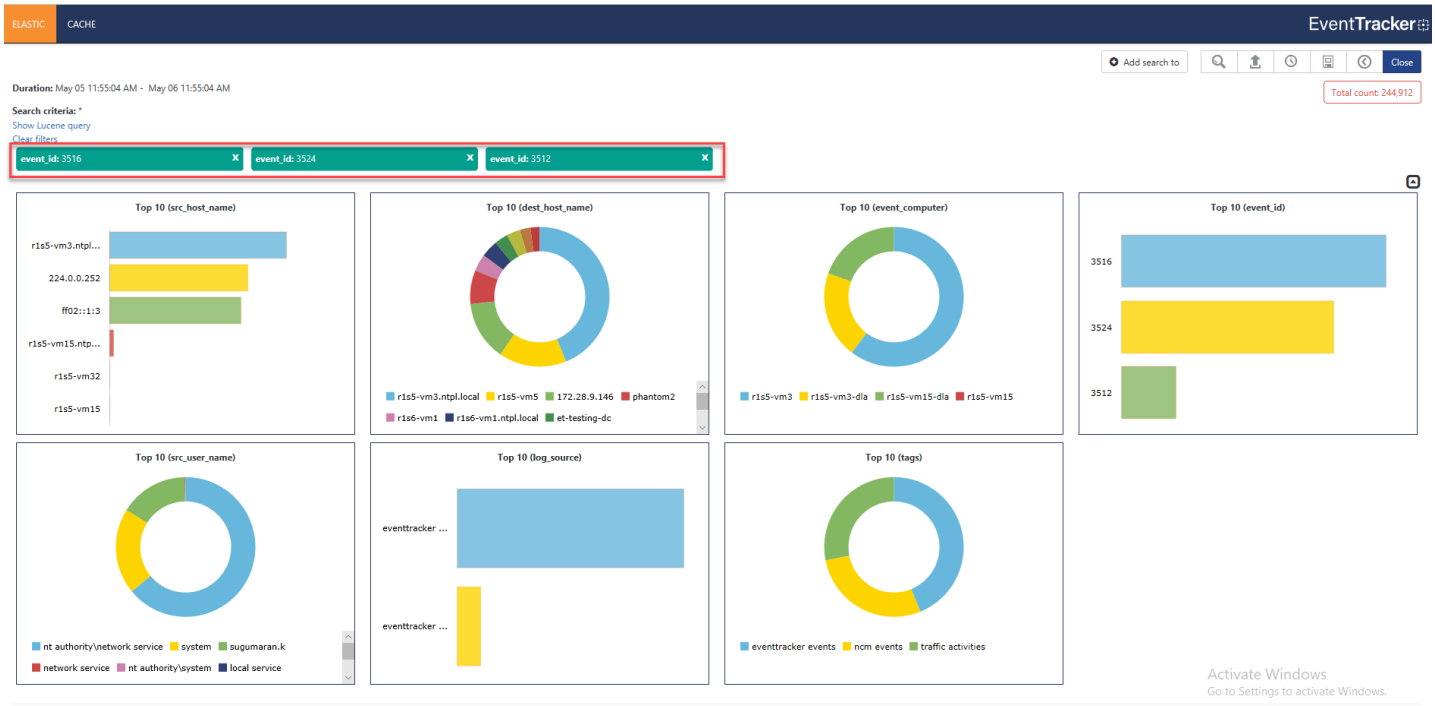

Figure 7

To exclude the values, in the result page.

1. Click the **View field values** icon for the "**event_id"** CIM field.

Figure 8

2. Choose the values from the "**Values for event_id"** dialog box window and click **Exclude** option.

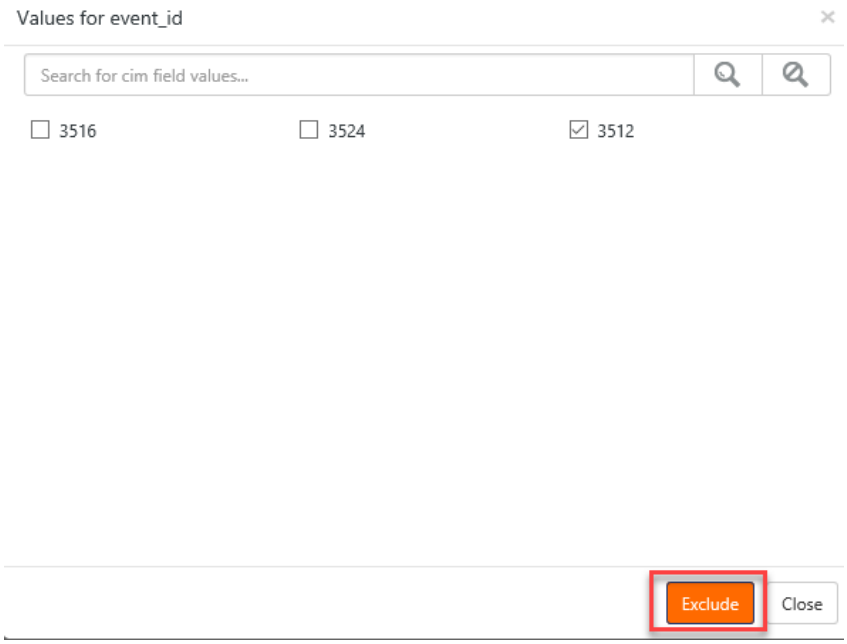

Figure 9

3. The excluded value is highlighted in orange color.

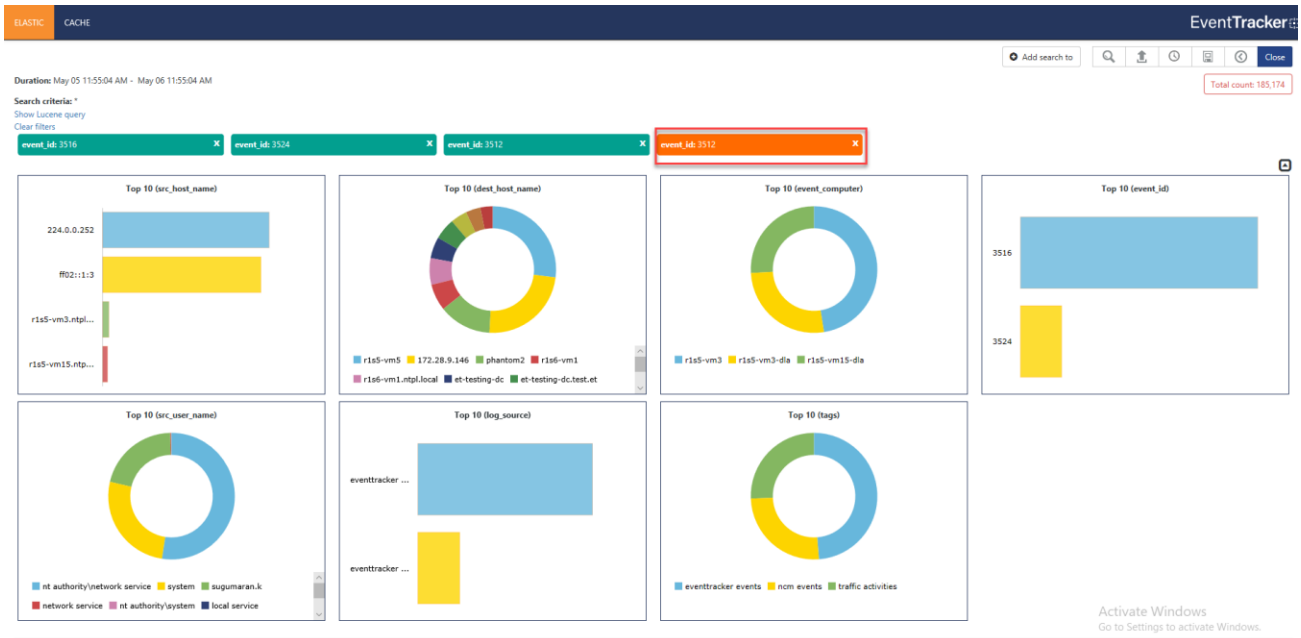

Figure 10

NOTE: The same changes apply for both Cache Search and Archive search.

Option to move systems from one group to other in System Manager.

User is provided with an option to select the system and move to any other groups.

To move the system to other groups.

1. Click **Admin** option from the Home page and choose Systems.

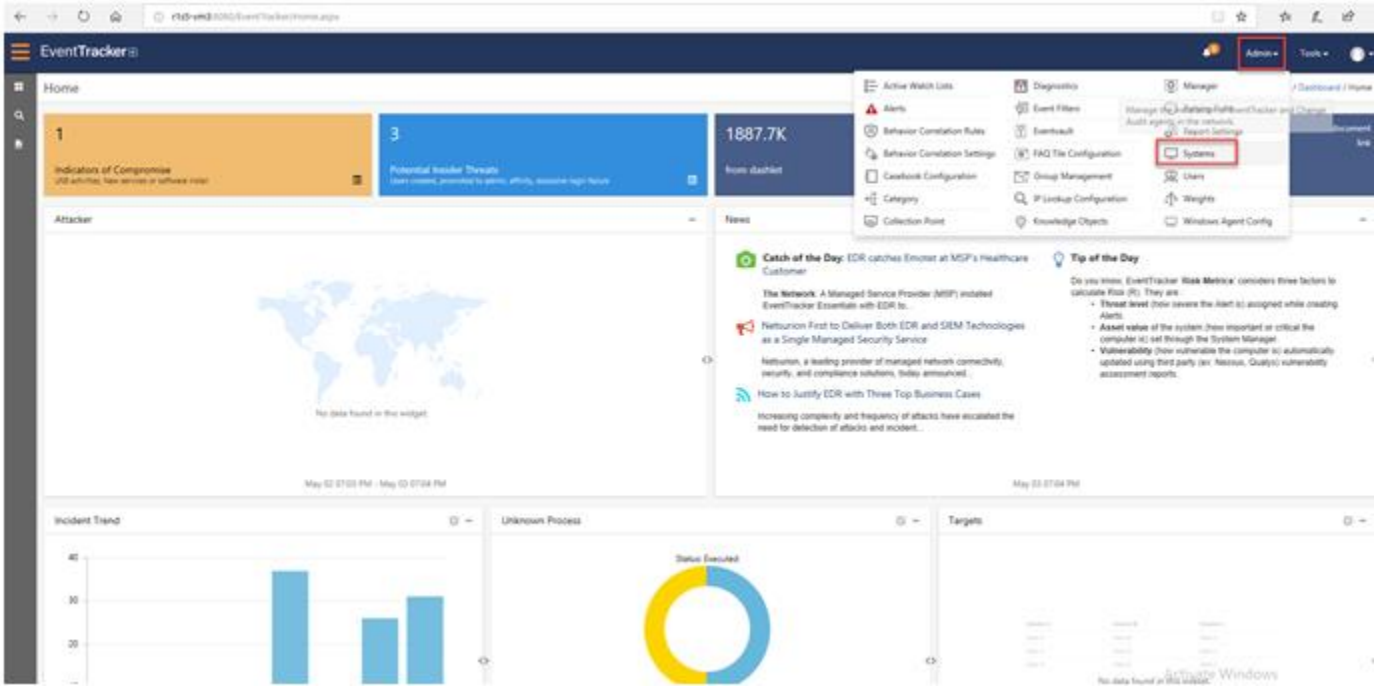

Figure 11

2. In the Systems Manager Page, click **Groups** icon.

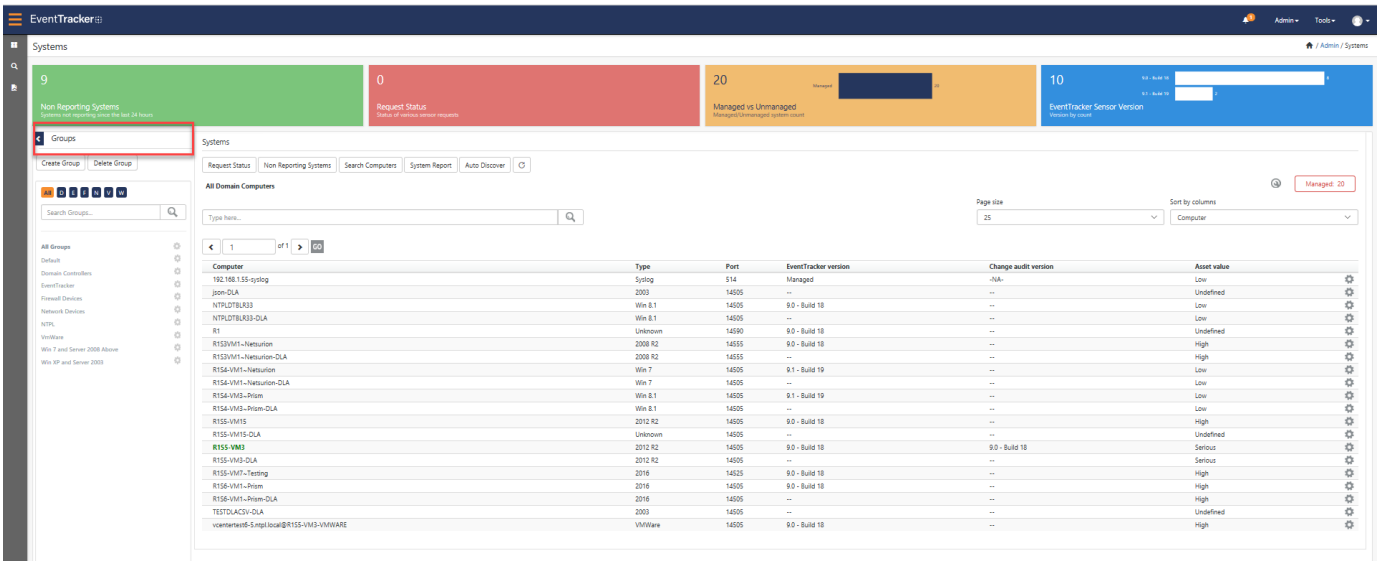

Figure 12

3. Click **Tools** icon and choose **Move System** option.

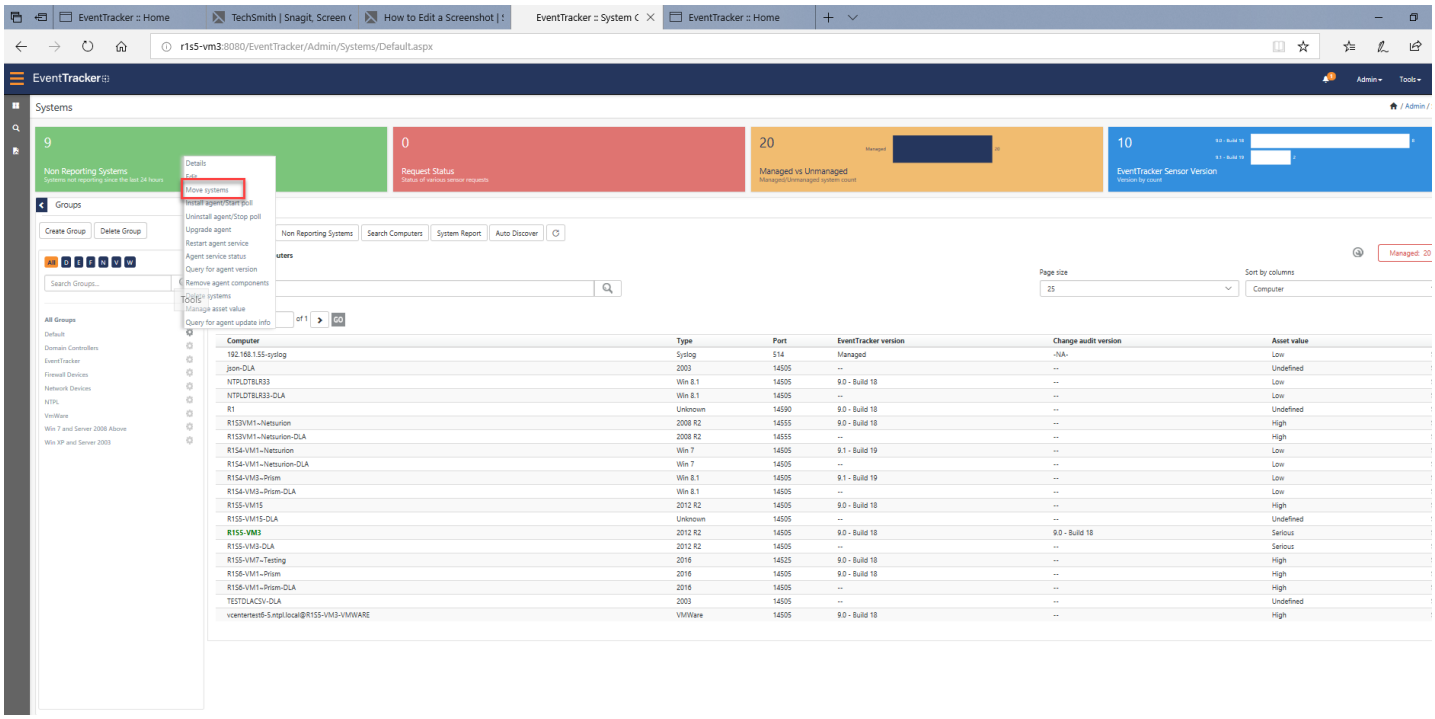

Figure 13

4. **"Move Systems from group"** window opens.

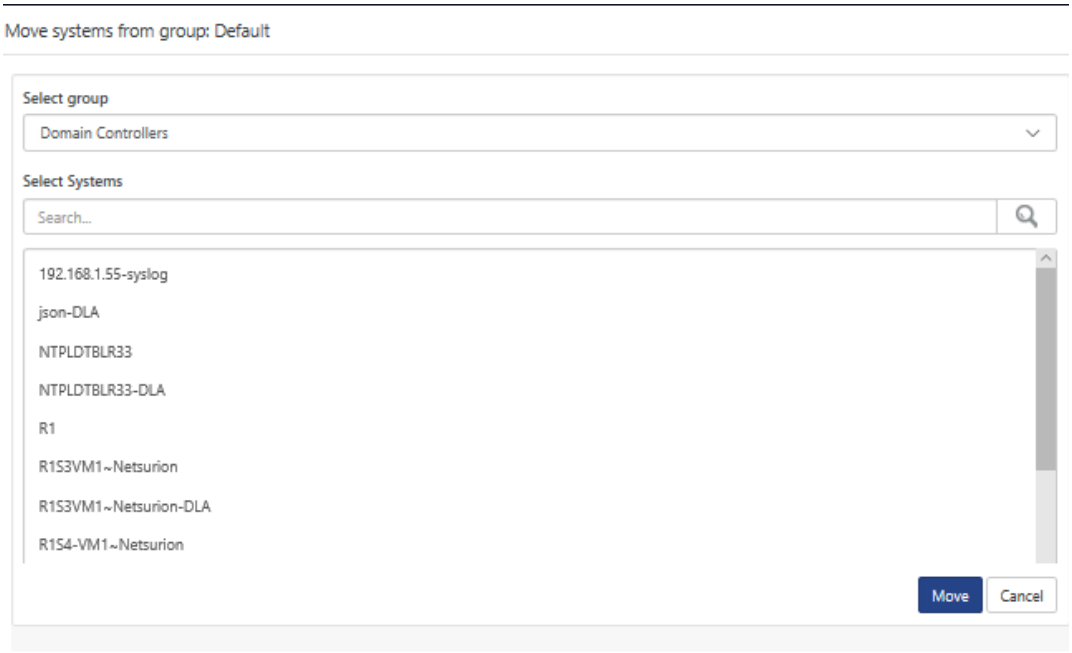

Figure 14

5. **Select Group** from the drop-down option you want to move from and **Select Systems** from the list.
6. Click **Move** button to move the systems from the selected group.